NIST Special Publication 500-163

NIST
PUBLICATIONS

Technology

U.S. DEPARTMENT OF
COMMERCE
National Institute of
Standards and
Technology

NIST

Government Open Systems Interconnection Profile Users' Guide

Tim Boland

The National Institute of Standards and Technology[1] was established by an act of Congress on March 3, 1901. The Institute's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Institute conducts research to assure international competitiveness and leadership of U.S. industry, science and technology. NIST work involves development and transfer of measurements, standards and related science and technology, in support of continually improving U.S. productivity, product quality and reliability, innovation and underlying science and engineering. The Institute's technical work is performed by the National Measurement Laboratory, the National Engineering Laboratory, the National Computer Systems Laboratory, and the Institute for Materials Science and Engineering.

The National Measurement Laboratory

Provides the national system of physical and chemical measurement; coordinates the system with measurement systems of other nations and furnishes essential services leading to accurate and uniform physical and chemical measurement throughout the Nation's scientific community, industry, and commerce; provides advisory and research services to other Government agencies; conducts physical and chemical research; develops, produces, and distributes Standard Reference Materials; provides calibration services; and manages the National Standard Reference Data System. The Laboratory consists of the following centers:

- Basic Standards[2]
- Radiation Research
- Chemical Physics
- Analytical Chemistry

The National Engineering Laboratory

Provides technology and technical services to the public and private sectors to address national needs and to solve national problems; conducts research in engineering and applied science in support of these efforts; builds and maintains competence in the necessary disciplines required to carry out this research and technical service; develops engineering data and measurement capabilities; provides engineering measurement traceability services; develops test methods and proposes engineering standards and code changes; develops and proposes new engineering practices; and develops and improves mechanisms to transfer results of its research to the ultimate user. The Laboratory consists of the following centers:

- Computing and Applied Mathematics
- Electronics and Electrical Engineering[2]
- Manufacturing Engineering
- Building Technology
- Fire Research
- Chemical Engineering[3]

The National Computer Systems Laboratory

Conducts research and provides scientific and technical services to aid Federal agencies in the selection, acquisition, application, and use of computer technology to improve effectiveness and economy in Government operations in accordance with Public Law 89-306 (40 U.S.C. 759), relevant Executive Orders, and other directives; carries out this mission by managing the Federal Information Processing Standards Program, developing Federal ADP standards guidelines, and managing Federal participation in ADP voluntary standardization activities; provides scientific and technological advisory services and assistance to Federal agencies; and provides the technical foundation for computer-related policies of the Federal Government. The Laboratory consists of the following divisions:

- Information Systems Engineering
- Systems and Software Technology
- Computer Security
- Systems and Network Architecture
- Advanced Systems

The Institute for Materials Science and Engineering

Conducts research and provides measurements, data, standards, reference materials, quantitative understanding and other technical information fundamental to the processing, structure, properties and performance of materials; addresses the scientific basis for new advanced materials technologies; plans research around cross-cutting scientific themes such as nondestructive evaluation and phase diagram development; oversees Institute-wide technical programs in nuclear reactor radiation research and nondestructive evaluation; and broadly disseminates generic technical information resulting from its programs. The Institute consists of the following divisions:

- Ceramics
- Fracture and Deformation[3]
- Polymers
- Metallurgy
- Reactor Radiation

[1]Headquarters and Laboratories at Gaithersburg, MD, unless otherwise noted; mailing address Gaithersburg, MD 20899.
[2]Some divisions within the center are located at Boulder, CO 80303.
[3] Located at Boulder, CO, with some elements at Gaithersburg, MD.

NIST Special Publication 500-163

Government Open Systems Interconnection Profile Users' Guide

Tim Boland

National Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

August 1989

NOTE: As of 23 August 1988, the National Bureau of Standards (NBS) became the National Institute of Standards and Technology (NIST) when President Reagan signed into law the Omnibus Trade and Competitiveness Act.

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Raymond G. Kammer, Acting Director

NIST

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) (formerly the National Bureau of Standards) has a unique responsibility for computer systems technology within the Federal government. NIST's National Computer Systems Laboratory (NCSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. NCSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. NCSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 500 series reports NCSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

Library of Congress Catalog Card Number: 89-600749
National Institute of Standards and Technology Special Publication 500-163
Natl. Inst. Stand. Technol. Spec. Publ. 500-163, 146 pages (Aug. 1989)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1989

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.0 INTRODUCTION

1.1 Welcome

Welcome to the world of the Government Open Systems Interconnection Profile (GOSIP). Open Systems Interconnection (OSI) is a revolutionary concept in data communications whereby computer systems are able to communicate in an open environment without knowledge of specific characteristics of remote host computers. The OSI approach makes possible a wide degree of interoperability between a variety of computers manufactured by different vendors.

The benefits of OSI for the U.S. Government are (1) effective, interoperable networking solutions saving money and providing increased communications capability, (2) minimal additional networking related software development costs, and (3) competitive products marketed on a worldwide basis by U.S. computer vendors. These benefits may be realized via GOSIP [NIST 2]; both GOSIP and OSI will be explained in this document.

OSI concepts are expected to drastically alter the Federal workplace for the user in the 1990's. These concepts satisfy a need that has been perceived since the early 1970's, when it was recognized that a lack of interoperability among heterogeneous systems would not be of benefit to U.S. Government integrated applications in the near future. The progression of the OSI effort is as follows: (1) development of international standards, (2) vendor and user agreements based upon these standards, (3) development of OSI communications products based upon these standards and agreements, and (4) development of tests for products showing conformance to the standards and demonstrating interoperability between products.

The importance of OSI concepts is manifest in the trend toward smaller, less expensive, and more powerful computer systems in today's world. Federal agencies are able to benefit greatly from OSI technology; GOSIP is a technical specification which gives detail necessary for Federal agencies to purchase OSI-based products and use them effectively.

Even though GOSIP provides essential information to benefit U.S. Government users, there is also additional information which needs to be provided to complete the GOSIP assimilation process. This GOSIP Users' Guide attempts to fill this gap in information and complete resolution of outstanding issues; it is meant to be a service and aid to the user.

1.2 Nature and Purpose of Guide

The expected audience for this Guide is: (1) Federal procurement specialists (or their agents), (2) Federal technical specialists, and (3) Federal management. By consulting this Users' Guide, Federal procurement personnel learn how to purchase GOSIP products, and Federal technical personnel learn how to evaluate those products for technical merit. Federal management is also interested in the technical issues, but also learns how to develop project plans and goals around GOSIP by using this Guide.

This Guide consists of short, diverse sections each designed to assist the U.S. Government user in understanding and interpreting GOSIP technical information, and to enable the user to assimilate GOSIP-compliant products into the workplace. Each section addresses a different topic. There are certain sections which everyone should read; other sections may be read selectively (or in part).

For example, the Federal procurement person needs to be aware of acquisition requirements for GOSIP-compliant products. The Federal technical person needs to be acquainted with technical details relating to the installation, maintenance, operation, and evaluation of OSI products. The manager needs to plan and develop life cycle system strategies for reducing costs and increasing application effectiveness.

This Users' Guide is designed for the individual who has little or no experience in OSI implementations. Anyone with no previous exposure to OSI should be able to read and understand all portions of this Guide; however, the individual who has some experience in OSI may also gain insight from this Guide.

This Users' Guide serves as a companion document to the Federal Information Processing Standard (FIPS) 146, and is best used in conjunction with GOSIP and/or OSI documents. This Guide progresses from a general outline of the subject to specific detail. Appendix E contains a form the reader may use to provide comments, questions, and suggestions for improving later versions of the Users' Guide.

1.3 Brief History of OSI

The concept of OSI (Open Systems Interconnection) was developed to enable heterogeneous computer systems to interoperate in a data communications environment. This means that users on one host can communicate with users on another host without specific knowledge of the characteristics of the other machine.

To reduce design complexity, the OSI architecture is organized as a series of layers or levels, each one built upon its predecessor. Similar communications functions are contained in each layer. The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented.

Layer N (where N is 1,2,3,4,5,6 or 7) on one machine carries on a conversation with layer N on another machine. The rules and conventions used in this conversation are collectively known as the N layer protocol. The entities composing the corresponding layers on different machines are called peer processes. In other words, it is the peer processes at layer N that communicate using the N layer protocol. Figure 1 illustrates this scenario.

Some of the principles of the OSI Reference Model [ISO 1] are: (1) each layer performs a well-defined function, (2) minimal information flows across layer boundaries, and (3) internationally standardized protocols should be "derivable" from the functionality of each layer. The OSI Reference Model deals with communications functionality.

There are seven layers in the OSI Reference Model. These layers are referenced in the GOSIP FIPS. They are the: (1) Physical Layer, (2) Data Link Layer, (3) Network Layer, (4) Transport Layer, (5) Session Layer, (6) Presentation Layer, and (7) Application Layer. Each layer has a protocol specification, or a set of rules governing dialogue between peer processes (processes at the same level), and a service definition, which is associated with an interface to the next higher level. Each of the layers uses the service of the next lower layer; in turn each layer provides a service to the next higher layer (see fig. 2).

Layers 1 through 3 define machine-to-machine communication via intermediate systems. Layer 4 defines end-system to end-system communication, and layers 5 through 7 address user-oriented functionality. The interface definitions and the protocol layer definitions indicate that each layer may be modified independently of the adjacent layer, and that processes at a certain layer need not have detailed knowledge of processes occurring at other layers. Many references are made to these concepts in the GOSIP FIPS; for additional information, readers may look in Appendix A of this Guide, which will give tutorial material on OSI. Specific publications referenced in Appendix B will also guide the reader in an introduction to OSI.

Though much work remains to be done, standards are now in place for the entire seven layers, and the focus is on developing products based on OSI that the user can use. In this regard, GOSIP was developed to enable the Government to take advantage of the emerging OSI technology.

Work done by implementor groups, such as the MAP TOP group (see sec. 3) and the NIST Workshop for Implementors of OSI (see sec. 3), serves to further define OSI in the context of specific systems and applications. Demonstration events which have taken place (e.g., National Computer Conference, 1984, and Autofact, 1985) serve to highlight accomplishments and to provide a practical forum to illustrate the workability of OSI in a practical sense. The Enterprise Networking Event (ENE) in June 1988 was the first major OSI product exhibition. For additional material on the relationship of the OSI development environment and GOSIP, refer to section 3 of this Guide

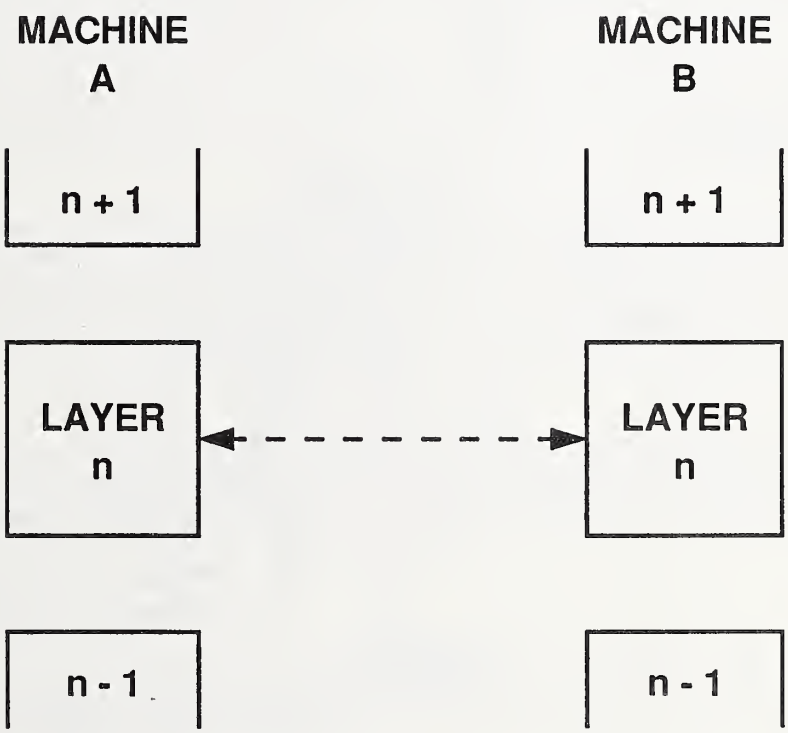


FIGURE 1
OSI COMMUNICATION

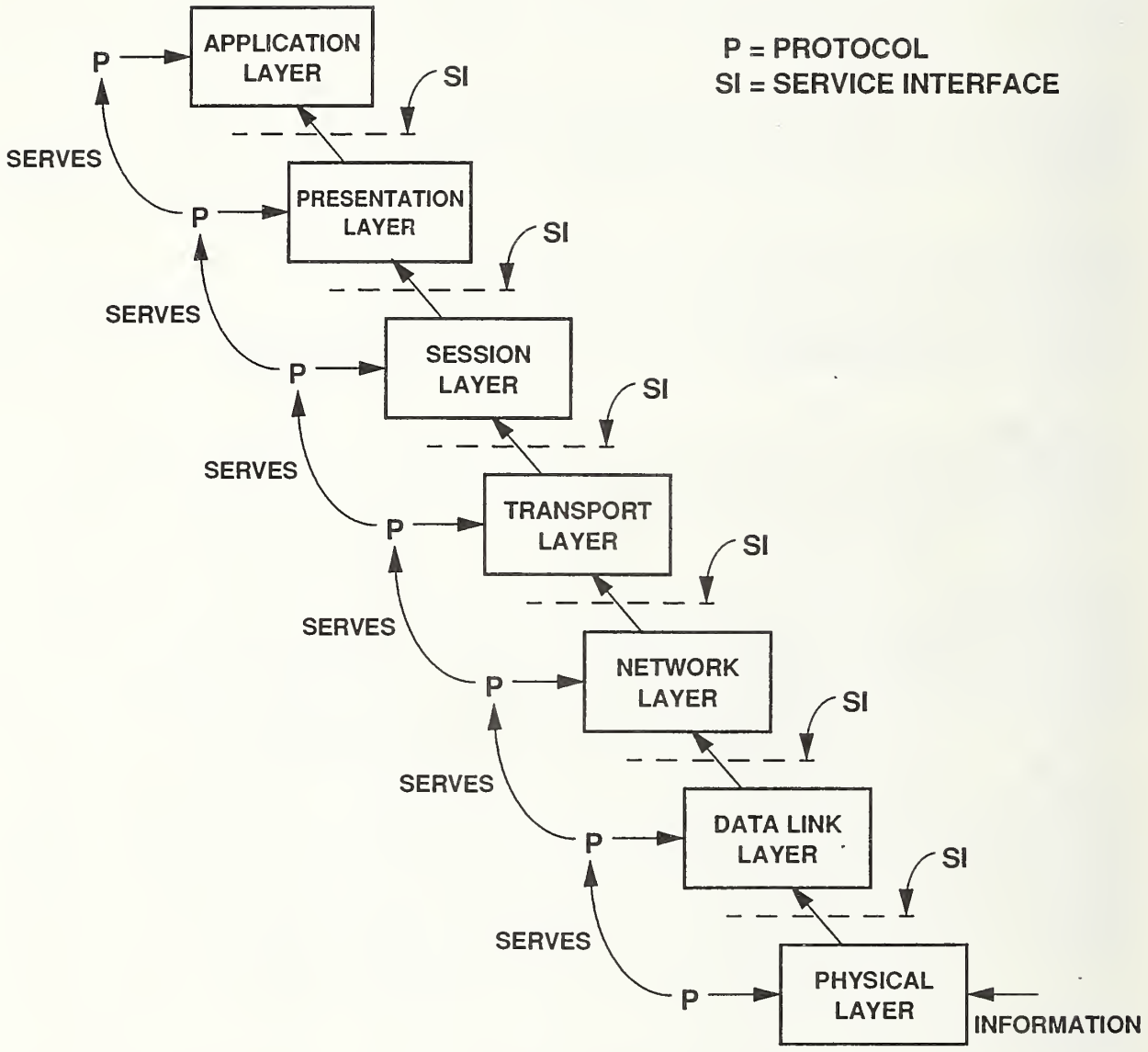


FIGURE 2
OSI LAYERING DEFINITION

1.4 Role of GOSIP

GOSIP is a result of a desire to simplify and ease the process of assimilating OSI technology into Federal agencies by: (1) specifying a common generic set of requirements (to avoid having users independently consult a plethora of complicated standards), and (2) ensuring stability in OSI material referenced in Federal procurement efforts. Version 1 of GOSIP is a technical specification which contains a core set of protocols and services; future versions of GOSIP will contain additional functionality.

A Federal agency may have hundreds of disparate information systems which are not interconnected and which include products from virtually every vendor. The resulting heterogeneous environment may exhibit a high degree of incompatibility in terms of hardware, software, data, and communications. This incompatibility may lead to problems such as inefficiency, poor performance, high expense, and a general feeling that things are out of control. It is problems such as these which GOSIP is designed to correct.

GOSIP defines and describes a common set of data communications protocols which enable systems developed by different vendors to interoperate and enable the users of different applications on these systems to exchange information. These protocols were developed by international standards organizations, primarily the International Organization for Standardization (ISO) and the Consultative Committee for International Telegraph and Telephone (CCITT). GOSIP is based on agreements reached by vendors and users of computer networks participating in the National Institute of Standards and Technology (NIST) Workshop for Implementors of Open Systems Interconnection.

GOSIP specifies a subset of OSI protocols, and may be described as a selection of a limited number of OSI protocols from each layer of the OSI Reference Model, as appropriate. Such selection is necessary for procurement reasons.

GOSIP is to be used by Federal Government agencies when acquiring computer network products and services and communications systems or services that provide equivalent functionality to the protocols defined in GOSIP documents. For the indefinite future, agencies will be permitted to buy network products in addition to those specified in GOSIP and its successor documents. Such products may include other non-proprietary protocols, proprietary protocols, and features and options of OSI protocols which are not included in GOSIP.

The appendices to the GOSIP specification describe advanced requirements for which adequate profiles have not yet been developed. Federal government priorities for meeting these requirements and the expected dates that work on these priorities will be completed are also provided. More information on each of these subjects is given in section 7.

1.5 Format and Layout of Guide

Section 1 provides background and introductory material. Section 2 provides an overview of the benefits of OSI from different perspectives (economic, functional, and planning); this section should be read by those interested in the motivation for this effort.

Section 3 gives a perspective on how protocols mature and are included in GOSIP. The relationship of GOSIP to other OSI-based documents and how GOSIP advanced requirements will be included in future GOSIP releases is also specified.

Section 4 contains a list of commonly asked questions about the GOSIP FIPS, with corresponding answers. This is of benefit to users who desire a quick introduction to or a quick summary of GOSIP.

Section 5 gives a general statement of GOSIP applicability to Federal ADP environments. Also included is a description of the waiver management process, GOSIP enforcement issues, and additional recommendations and considerations for GOSIP applicability.

Section 6 gives information on strategies that agencies should use to procure GOSIP-compliant products and services. This section should be read by Federal procurement personnel.

Section 7 provides insight into technical aspects of OSI communications, enabling proper evaluation of GOSIP products. This section should be read by technical personnel and managers, and provides supporting documentation for the procurement process elaborated in the previous section.

Section 8 describes objects which need to be registered, and gives instructions on how to register these objects. This section should be read by all system managers and technical managers. Future registration issues are also discussed.

Section 9 gives information on life-cycle management; this section includes recommendations for planning and executing generic transition strategies from proprietary systems to OSI-based systems. Some detailed case histories are given mentioning plans that may be used for particular situations.

Section 10 provides references on other programs which may interact with GOSIP systems in the near future (FTS2000, POSIX, CALS, EDI). There are a variety of standardization activities taking place in the Federal sector in the near future, and it is important that managers and planners keep track of developments.

Appendix A gives detailed tutorial information on OSI and some important components (including File Transfer, Access and Management; and Message Handling Systems applications). Users desiring additional knowledge of OSI and related topics should read Appendix A. Appendix B gives points of contact and additional reference material for those wishing more information. Appendix C gives sample forms to be used for GOSIP OSI registration (see sec. 8). Appendix D gives a list of participants in an important OSI-related activity (see sec. 3.2.2). Appendix E, as mentioned previously, consists of a form to be used for comments, questions, and suggestions.

In summary, procurement personnel should read sections 1, 5, 6, and 10; executives should read sections 1, 2, 4, and 10, and technical personnel should read sections 3, 7, 8, and 9. However, Federal agency personnel who need to know more about the GOSIP process and protocols are encouraged to read all sections of this Guide.

1.6 Acknowledgments

The author wishes to thank the personnel at the National Institute of Standards and Technology who assisted in the preparation of this Guide, including Jerry Mulvenna, Kevin Mills, Dale Walters, Doug Montgomery, Richard Colella, and Shirley Radack, among others. Other personnel from various Government agencies who have assisted in various portions of this Guide are: Bruce McLendon of NASA, Ray Denenberg of the Library of Congress, Jerry Cashin of the Air Force Computer Acquisition Center, Jerry Gibbon of the Department of Commerce, Robert Buckley of the Navy Department, and Leon Blue of the State of Florida, among others.

2.0 OVERVIEW FOR EXECUTIVES

2.1 Introduction

GOSIP is expected to dramatically alter the way the Federal Government purchases ADP communications technology. In order for maximum benefit to be gained from this new technology, strategic planning initiatives should be developed now at the highest echelons of Government. In order for this to happen, Government executives must be informed of the long-term benefits of OSI technology, and be assured that this technology is relevant to their agency. Accordingly, benefits will be presented from planning, functionality, and economic perspectives.

The benefits of standardization to the U.S. Government are many, for both the user and the vendor. Users may choose the best network solutions without being locked into a specific vendor. Small- to mid-sized vendors may effectively compete in the open marketplace. A wide variety of products will be available soon. This section introduces the Federal executive to the advantages of incorporating GOSIP-compliant systems into the Federal ADP environment.

Imposition of GOSIP will encourage competitive procurements and facilitate development of centralized agency policies relating to data communications procurement. A kernel set of capabilities exists in OSI products; this set will become much larger over time, promoting multi-vendor interoperability. OSI products are based upon technically stable standards and agreements (see sec. 3). Furthermore, a world market is being created for OSI products, so that vendors should be able to sell not only to the U.S. Government, but also to other users in America and around the world.

GOSIP allows users the ability to incorporate standard and nonstandard communications facilities in such a way as to promote interoperability and connectivity. The aim of OSI standards is to facilitate the accomplishment of user objectives through the incorporation of state-of-the-art communications technology. The level of commitment of agency resources to incorporate OSI products need not be large over the long term, and it is possible to move to the OSI environment with a minimum of disruption, as is being illustrated by the Department of Defense.

To the executive, this means that project plans may proceed along predictable lines; agency heads should be able to plan system upgrades within system interoperability limits with confidence. Manpower and human resources can be saved and program goals need not be sacrificed for computer and system limits. Agency heads can satisfy program objectives and be guaranteed support from data processing facilities. In short, adopting OSI as a strategic policy will ultimately lead to improved information transfer within an agency, with attendant benefits.

2.2 Economic Benefits

Projected cost savings over the life cycle of a GOSIP system, when contrasted with alternative choices, may be substantial; furthermore, the longer the life cycle, the greater the savings. This is due to several factors described below.

First, small- to mid-sized vendors can market OSI products competitively with larger vendors. Since more vendors can compete for a share of the market, total projected costs for the consumer should be reduced. As with any supply-and-demand situation, a larger number of vendors entering the market means the price for the customer may be minimized, because of the increased competition. The larger the number of vendors entering the competitive procurement process, the lower the final prices are likely to be.

The second factor is implementation variety. GOSIP-compliant products are expected to be offered and designed to vary in price. Increased competition and resultant lowered final prices may enable customers to choose the best network solution based upon user needs.

The third factor keeping prices down is the avoidance of excessive software development costs. The

cost of hardware in general is expected to remain fairly stable over time; software costs are expected to continue to rise dramatically over the next several years. Software development is a "human intensive" effort requiring large numbers of people as well as training and management expertise. The implementation of GOSIP tends to reduce these costs. Communications software development is minimized because GOSIP relies on an open communications architecture, whereby machines are able to interoperate without need of sets of special purpose software to connect each machine to each of the other machines on the network.

The fourth major factor keeping costs down is that interoperability of aging OSI equipment with evolving OSI equipment is possible when following GOSIP; thus, an agency is able to avoid expensive purchases of computer equipment in the future to achieve a certain level of communications functionality and interoperability. Users may cost effectively switch to lower-cost or higher-performance vendors without losing GOSIP interoperability.

The final major factor is that establishment of a standard architecture like that referenced in GOSIP allows a hardware base upgrade without losing the investment in software. A customer is able to add new hardware components to existing systems without the requirement to purchase expensive new software. A GOSIP-compliant solution for interoperability is likely to be less expensive than a special custom-designed solution for a particular configuration.

Some other cost saving factors of OSI products must be mentioned as well. The modular approach to OSI design enables modifications to be made more efficiently. Also, once an initial OSI training period is past, future training and overhead costs should be relatively low.

In sum, acceptance of OSI technology offers substantial cost savings that should grow over the life cycle of the system. Furthermore, these savings are largely predictable, in the sense that vendors are able to meet with an agency to develop long-term solutions which will minimize long-term costs.

2.3 Functional Benefits

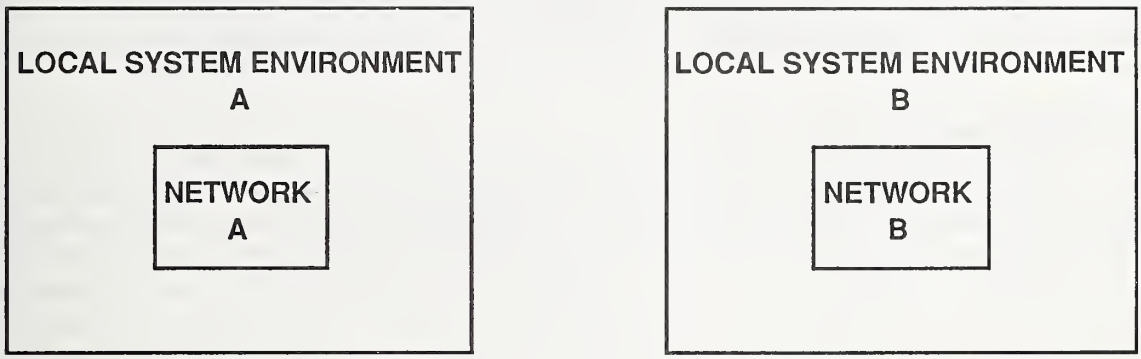
Functional benefits of OSI implementation are as follows: (1) interoperability without loss or compromise of local system environments (user interfaces), (2) enhanced services available with OSI applications, (3) a growth in capabilities over the next few years, (4) the selection of options and features that best satisfy a stated need, and (5) a reliable end-to-end transfer service over which standard and nonstandard applications may be written. Each of these benefits is explained in some detail below.

For (1), the adoption of a standard architectural solution for interoperable data transfer allows existing and future networks to be interconnected, thus enabling users on one network to communicate effectively with users on other networks. This can be accomplished without the need for a vendor to modify existing user interfaces, because there is no need to do so to achieve multi-vendor interoperability. Thus a vendor may add GOSIP-related services while preserving special end-user services. The above-described scenario is illustrated in figure 3. As as example, GOSIP electronic mail protocols may be used to interconnect individual electronic mail systems.

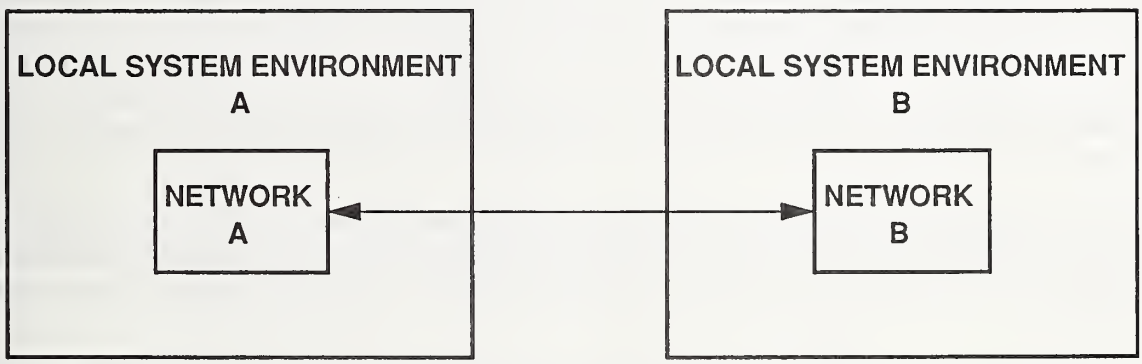
For (2), in general, GOSIP applications offer many services and features not found in many current products. The GOSIP electronic mail service gives users additional capabilities not found in many current mail systems, without losing capabilities found in these current systems. The GOSIP file transfer service gives users many functional benefits not found in current file transfer systems. Future GOSIP applications are expected to offer similarly enhanced capabilities over current systems in the appropriate functional areas.

For (3), it is expected that a large number of additional capabilities will be provided in GOSIP in the near future. The number of OSI-based services available to the user should increase accordingly.

For (4), multi-vendor competition means that a user can differentiate and choose OSI products based on specific features and options that best satisfy a user's functional requirements; thus, a product can be custom-designed to satisfy particular user wishes while satisfying GOSIP requirements. Furthermore, the



a) BEFORE



b) AFTER

FIGURE 3
INTERCONNECTION SCENARIO

OSI architecture allows for options that may be used in this way.

For (5), the GOSIP provides for a reliable end-to-end transfer capability. This capability is able to support many different applications and user environments. Users may write or buy their own applications to exploit this capability.

In sum, the increased scope of existing applications and network configurations and the increased power of these same applications and configurations can allow more productive work to be accomplished in a shorter period of time. A number of capabilities are expected to be provided in OSI products that have not been provided previously. In addition, current OSI capabilities are state-of-the-art, and represent the latest advances in networking technology. GOSIP is bringing up-to-date communications knowledge, technology, and products to Federal agencies.

2.4 Planning Benefits

There are a number of administrative and planning benefits available to executives when OSI technology is implemented, and when a GOSIP direction is set. The emergence of GOSIP means that agencies should be able to predict expenses in the future for procurement, upgrades, manpower, future resource allocations, and future capabilities. This is because the OSI concept allows for a steady development and progression of capability which is based upon backward compatibility and widening interoperability. An agency may add resources and capability gradually, or rapidly, depending on preference. Throughout the life cycle of a system, the need for unexpected, large purchases should be diminished.

The increased interoperability possible with OSI products means that diverse networks are connected, and different centers of network control and management may be consolidated into one level of control. This should allow for simplified configuration management, and much simpler control planning. Agency-wide policies may be set up governing computer use, and computer resources across an agency can be managed from a central location. Paperwork and human resources can be reduced. Again, a single policy can be established for an agency covering communications, and can remain in force for the indefinite future. Control over networking capabilities can be exercised from a single point. It should be easier to plan long-term ADP procurements.

In terms of program management, instead of a compendium of different programs, each dependent upon a particular underlying communications capability, there can be a single set of programs covering the entire agency. Agency programs can be adapted to seek input from other agencies involved in inter-agency communication.

Finally, adoption of GOSIP allows agencies, to a greater extent, to develop policies that are independent of any particular ADP environment. Agency programs should serve the user, based upon the user's stated needs; the use of GOSIP in procurement can enable those needs to be more directly met. More attention from a planning perspective may be paid to what service an agency is providing according to its mission, and not to the complex details of how that agency operates in meeting its commitments from a computer-related standpoint.

In sum, the adoption of GOSIP means that agencies can have a much greater degree of control over long-term planning. Cost and resource projections may be given far into the future with confidence. This can increase overall agency efficiency, and allow an agency to concentrate to a greater extent on long-term program priorities, rather than on communications capability.

2.5 Summary and Direction

A comprehensive set of benefits to be gained by using OSI technology was explained above. It should be apparent at this point that adopting OSI as the key data communications strategy now and in the future is a wise idea. Such adoption can assist agencies in meeting their program goals now and in the future more efficiently and less expensively than would otherwise be possible.

In light of the above discussion, what is the next step for an agency executive? The answer is that a comprehensive strategic initiative should be developed at the highest levels of an agency at the earliest possible time. If possible, such a strategy embracing the OSI concept should be formally adopted as specific agency policy. The U.S. Congress, the Office of Management and Budget, the Department of Commerce, and the Department of Defense have all endorsed the concept of OSI and GOSIP.

A long-term commitment should be made by agency executives to support GOSIP in all future networking decisions. This commitment should be clear and unambiguous, and should have the support of the highest ranking officer of an agency as a public declaration. Once a future networking decision based on OSI is set, vendors should be notified, specific transition plans should be developed, and orderly integration of OSI products into the appropriate Federal work environments can begin. The DOD has already endorsed GOSIP at the policy level, and has issued an OSI implementation plan.

In summary, an agency executive should examine specific programs, organizations, and goals within the agency to determine how the above-mentioned benefits of GOSIP can best be realized. A clear focus should be established; the question "What should the status be of agency communications at a specified point in the future?" should be answered. Appropriate support personnel should be consulted in this regard. Other sections of this Guide give specific assistance in moving forward toward OSI integration once a definite policy is in place.

3.0 PERSPECTIVE ON GOSIP

3.1 Introduction

This section gives a perspective on the GOSIP process. The benefits of OSI are numerous, as previously described. The promulgation of GOSIP as a FIPS represents a major accomplishment in bringing OSI technology into the Federal workplace. A number of steps were necessary to reach this advanced point, and they are described below.

The inclusion of specific OSI communication protocols and services into GOSIP is no accident. There is a deliberate, organized process by which this work matures and becomes useful. The pace of development of OSI work may seem relatively slow, but this is to ensure that the work in place is stable. There is another time factor at work, however, as reflected in the desire for users to see marketable OSI products as soon as possible. The creation of a user market drives the vendors and gives impetus to the OSI development effort. In turn, the vendor must be convinced that users will buy OSI products; thus, vendors and users continue to give impetus to each other in the push for worldwide interoperability.

There are several characteristics common to all of the protocols referenced in GOSIP. These are: (1) wide applicability (generally useful not only to U.S. agencies, but on a worldwide basis), (2) availability (implementations exist now or will be available in the near future), (3) stability (protocols are technically "frozen" and are not expected to change in the foreseeable future), and (4) effectiveness (the protocols will solve a common need of the Federal agencies). In addition, vendors and users alike must agree on marketing and transition strategies to integrate this technology into the workplace.

3.2 Steps to GOSIP

Below are given some of the critical steps in OSI development, from recognition of need to development of an environment in which GOSIP was created.

3.2.1 Standards Development

The beginning of the process is the recognition of deficiencies in some aspect of communications. For example, file formats on dissimilar systems may be completely incompatible, but may need to be integrated in one large application. The overall lack of interoperable configurations is a general problem, emphasized previously in this document.

In the early 1970's, as knowledge of computer networking increased, the potential and problems in its use became apparent. By the late 1970's, lack of interoperability and lack of compatibility between different machines posed significant problems in data communications. Users were "locked" into specific vendor solutions, local software development costs were high, small vendors could not market products competitively worldwide, and so on. In order to interoperate in the 1970's, a specialized interface had to be developed between any two machines; as the number of machines grew, so did the number of required interfaces, to an unacceptable level.

This is the general problem. To solve this problem, the Defense Advanced Research Projects Agency (DARPA) of the Department of Defense (DOD) developed a nonproprietary set of protocols that would allow different machines to communicate more efficiently and effectively. The DARPA protocols [DOD 1-2] represented a major advance in this direction, and the DOD protocols were mandated in 1982 for DOD-wide use. A National Research Council (NRC) study [MISC 3] has recommended that the DOD evolve to use OSI protocols, and the DOD has subsequently endorsed the OSI concept [DOD 3].

In the late 1970's, the International Standards Organization (ISO) developed a common reference model which partitioned the functions involved in data communications into seven layers. Committees and subcommittees were formed, and the work of developing standards for the seven layers began. Vendors and users provided input into the process, based upon real-life experiences and concerns. These meetings were

(and are) open to all interested participants.

Independently of the ISO, the Consultative Committee for International Telegraph and Telephone (CCITT) began work on telecommunications-based interoperability standards in Europe. Due to the need for commonly defined and supported telecommunications-based capabilities, work progressed rapidly toward a set of agreements also based on the OSI architecture.

In 1979 the National Bureau of Standards (NBS) (now the National Institute of Standards and Technology (NIST)) initiated a program to support creation of standards that would meet U.S. Government needs for interoperable data communication. Since then, the NIST has actively encouraged and promoted the interests of Federal users in the ISO and CCITT standards development effort, and the resulting standards reveal this influence. The process desribed below is preserved in standards development today.

The early work of the ISO and CCITT produced "rough" documents which are still somewhat technically unstable. Member bodies of the organizations improve these documents by successive cycles of comment, input, and review; along the way, new drafts are created, and are fed back into the process.

The result of this process is a stable document, which (in the ISO) is an International Standard (IS); in the CCITT, this document is a CCITT Recommendation. In the ISO, the progression is: Working Draft, Draft Proposal, Draft International Standard, and International Standard. In the CCITT this progression involves a 4-year program of work leading to a Recommendation. Member bodies in the United States are the American National Standards Institute (ANSI) for the ISO, and the Department of State for the CCITT. Figure 4 illustrates this arrangement.

In sum, key aspects of early standardization were: (1) the pioneering work of the DOD, (2) the telecommunications-based standards of the CCITT, and (3) the network-based standards of the ISO. The iterative processes described above continue today in further standardization.

At first the most immediate problems involving OSI "lower layer" technology (see sec. 7) were investigated. This is because it is important to specify error-free transmission before specifying user-oriented applications relying on such capabilities.

In the past several years stable standards have been completed (in both the ISO and the CCITT) for a "full" seven-layer OSI "stack". This was a necessary step in the development of OSI products. A list of these standards is given in Appendix B.

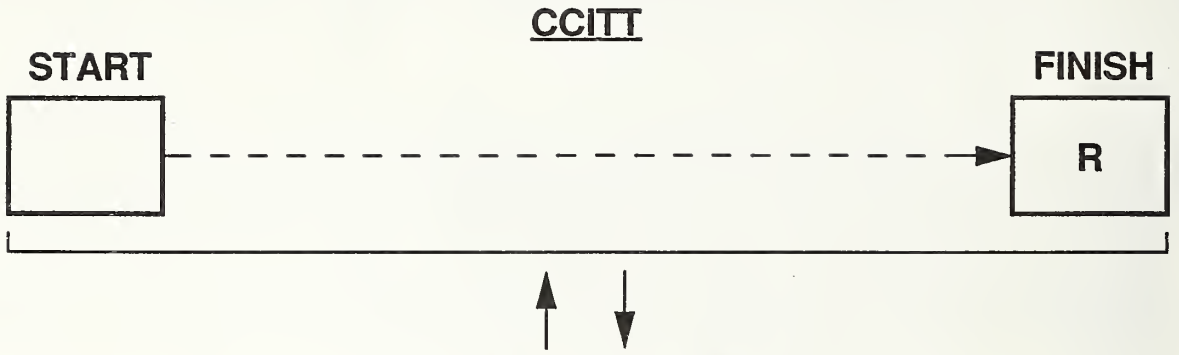
Work is now underway on additional standards such as network management and directory services. These are important additional services to be included in OSI products. Work is also underway on addenda to existing standards to improve their functional capability. Finally, additional applications are being standardized; these applications include a virtual terminal capability, office document transfer, and transaction processing. It is a design goal that this new work be built on the previous work, so that OSI products may be "upwardly compatible".

It is important to remember that whenever possible GOSIP is based upon stable international standards. Sometimes, it may be necessary to reference work in GOSIP that is not based upon stable standards. If this happens, it should be viewed as an attempt to develop an interim solution to a critical user requirement.

3.2.2 NIST/OSI Implementors' Workshops

Generic standards by themselves are not sufficient to specify OSI product capabilities. Such standards include a number of options, subsets, and unspecified implementation details. In order to specify the necessary additional detail, after the standards have been completed, vendors and users have convened at locations around the world in a series of OSI implementors' workshops.

The most prominent of these workshops is the NIST Workshop for Implementors of OSI, held in Gaithers-



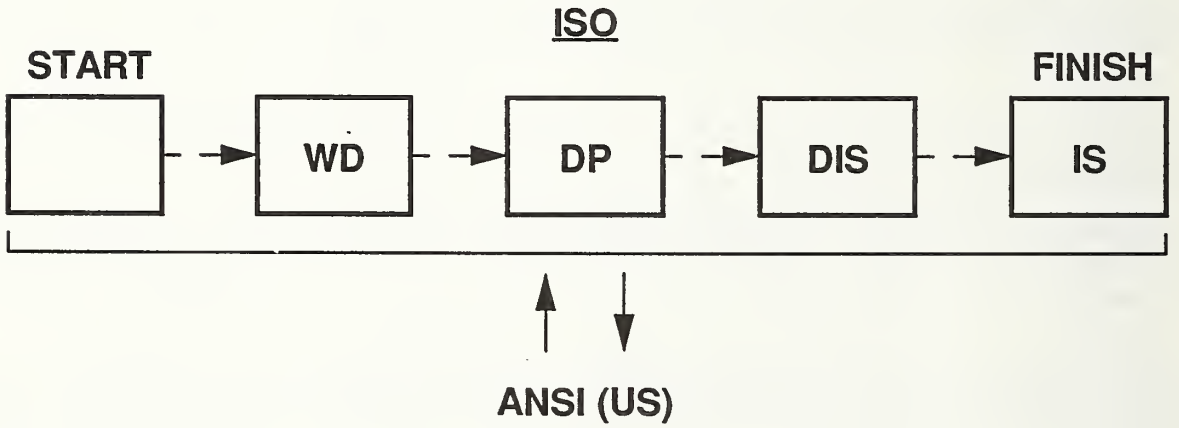


FIGURE 4
STANDARDIZATION PROGRESSION

burg, Maryland, at the National Institute of Standards and Technology (NIST). This workshop is held four times per year to enable vendors and users to reach detailed agreements on OSI implementation issues. This workshop has been in existence since February 1983, and is administered by NIST. These meetings are open to all interested participants. GOSIP is based upon agreements reached at these meetings, in addition to being based upon the OSI standards themselves.

All organizations that encourage the development of OSI standards and that plan to implement or buy OSI systems are invited to participate in the workshop. It is an established and effective mechanism for developing implementation agreements based on international OSI standards. This workshop is an open international forum, with participation of more than 200 computer manufacturers, semiconductor manufacturers, word processing vendors, process control vendors, communication carriers, and industry and government users from the United States, Canada, Europe, Australia, and elsewhere. The ultimate goal of the workshop is to promote OSI-based interoperability in multi-vendor environments.

Some typical computer and communications vendors participating in the workshop are: AT&T, Digital Equipment, Hewlett-Packard, IBM, and Unisys. Some prominent users participating in the workshop are Boeing, Department of Defense, General Motors, and the Veterans' Administration. For an expanded list of participating users and vendors, see Appendix D.

Documents of importance produced by the workshop are : (1) Stable Implementation Agreements for OSI Protocols, which gives implementor agreements that are not technically changing, (2) Ongoing Implementation Agreements for OSI Protocols (Stable), which gives agreements that are stable preparatory to inclusion in (1) above, (3) Ongoing Implementation Agreements for OSI Protocols (Continuing Agreements), which gives agreements that may be subject to technical change, and (4) the Workshop Procedures Manual, which governs the operation and conduct of the workshop meetings. In addition, there is a Style Manual. Release of the Stable Implementation Agreements for OSI Protocols ((1) above) occurs no more often than once per year.

A new version release of a stable document ((1) above) occurs to include new stable technical material. The ongoing document may include, in a special section or a separate volume, material which is technically stable and may be referenced in OSI product development, but which has not yet been included in the stable document. The stable document ((1) above) contains agreements which definitely may be used in OSI product development.

There are four important features of the workshop agreements. The first is that agreements are based upon stable ISO, CCITT, and other internationally recognized standards work as described in section 3.2.1. The second feature is that it is a goal for agreements to be "upwardly compatible"; that is, OSI products produced from one version will be able to interoperate correctly with OSI products from succeeding versions at the intersection of their capabilities. The third feature is that international harmonization and alignment efforts are underway with similar groups in other countries, with the goal of creating compatible worldwide implementation specifications. This would be of great benefit to both vendors and users. The fourth feature is that every attempt is made to reach agreements by unanimous consensus of all interested participants.

The NIST Workshop for Implementors of OSI organization is divided into a plenary and various Special Interest Groups (SIGs). Each SIG covers a different OSI functional study area. Each SIG is tasked by the plenary to do work under an approved charter, and submit this work to the plenary for ratification. Only work approved by the plenary is included in the stable and ongoing documents. The work must be of general benefit to vendors and users, and be related to the charter of the workshop (e.g., OSI communications). Information on the workshop, and copies of the above-mentioned documents, may be obtained from the National Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899 (ATTN: NIST Workshop for Implementors of OSI).

Version 1 of GOSIP is based on Version 1 of the NIST/OSI Stable Implementation Agreements (NBS SP 500-150) [NIST 1]. The creation of a stable set of workshop agreements is a necessary step toward the

assimilation of OSI products into the Federal environment. Hereafter the workshop will be referenced as the NIST/OSI Workshop, and SP 500-150 will be referenced as the NIST Workshop Agreements.

3.2.3 MAP and TOP

Vendors are marketing products based upon the above-mentioned standards and NIST Workshop Agreements. There need to be organizations that can effectively represent the interests of the various user communities in (1) making their requirements known to vendors, and in (2) stimulating the vendors to produce products based upon those stated user needs. A prominent example of such an organization is the MAP (Manufacturing Automation Protocol)/TOP (Technical and Office Protocols) Users Group. The MAP organization is concerned with factory automation communications support, and the TOP organization is concerned with office automation. These two organizations work together to promote user interests, and are largely functionally compatible. In turn, GOSIP seeks, where possible, to be functionally compatible with these two organizations.

The reasons for this collaboration are obvious. A single set of user requirements means that small and large vendors have a larger market to penetrate and that there is greater economic incentive for vendors to build interoperable OSI products.

Various public demonstrations of OSI implementations have been supported by MAP committees, including the National Computer Conference in 1984 and Autofact in 1985. The purpose of these demonstrations was (and is) to show the feasibility and workability of OSI. An Enterprise Networking Event in June 1988 was the first major exhibition of OSI-based communications products in the United States.

Although GOSIP has much in common with the goals of the MAP/TOP Users Group, there are differences which are reflected in the documents issued by the groups. The MAP [MISC 1] and TOP [MISC 2] specifications state what those organizations want the vendors to produce in the future to meet their requirements. GOSIP is mandated for use in Government procurement requests; for that reason GOSIP references functionality which is available from vendors now or in the near future. However, the protocols in GOSIP have been carefully coordinated with the MAP and TOP organizations in order to insure that vendors can produce implementations based on a single set of user requirements. For more information on MAP or TOP, write to:

North American MAP/TOP Users Group, P.O. Box 1157, Ann Arbor, MI 48106

3.3 GOSIP Summary

Federal Information Processing Standard (FIPS) 146 incorporating GOSIP has been issued by the NIST. The history, nature, scope, and future of GOSIP are described below.

In late 1986, as the standards, NIST Workshop Agreements, and MAP/TOP user specifications were nearing stability, an effort was initiated to develop a U.S. Government OSI profile. Vendor OSI implementations were being completed and demonstrated, and commercially-available OSI products were being produced. The intent was (and is) for U.S. Government users to take advantage of these developments. Figure 5 illustrates this progression.

Goals of the GOSIP effort are: (1) to enable Federal users to select optimal OSI protocols and options from among a wide variety of choices, (2) to define a single Federal user community to vendors, and (3) to transmit Federal user requirements to vendors, as well as to encourage vendors to build OSI products satisfying these requirements. The commitment of GOSIP is to achieve multi-vendor interoperability in the Federal workplace.

Through collaboration among a small group of U.S. Government technical experts, a draft specification was produced in December 1986. The GOSIP initial specification has undergone successive cycles of review and comment. All Federal agencies and interested organizations were invited to comment; these same

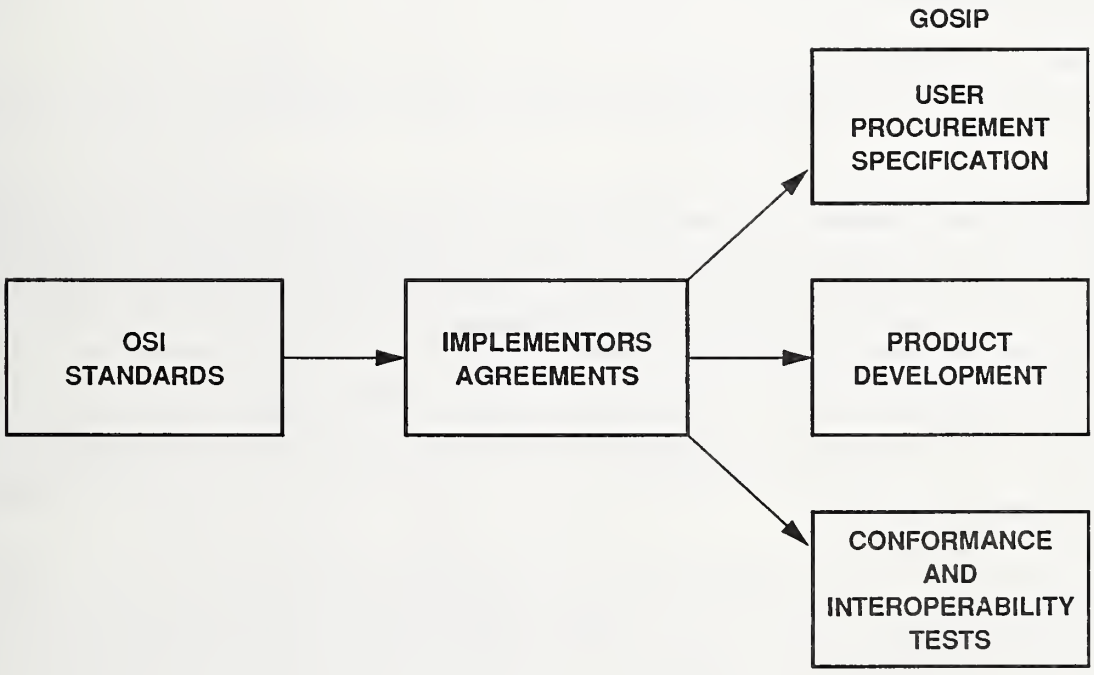


FIGURE 5
GOSIP CONTEXT

organizations provided valuable input back into the revision process. All segments of the U.S. Government were consulted during the preparation of this document.

The FIPS for GOSIP consists of two parts: (1) technical specifications (version 1), which contain information on the OSI protocols and services provided, and (2) information on applicability and implementation of the FIPS. After extensive government and industry review, GOSIP was promulgated as a FIPS (FIPS 146) in August 1988. GOSIP applies to all U.S. Government agencies around the world. Other organizations of a similar nature (e.g., State governments) may decide to adopt GOSIP for their programs as well. The NIST controls the contents of the GOSIP FIPS, with advice and consultation coming from other Federal agencies. Drawing on the technical contributions of these agencies, the NIST prepares GOSIP, has it reviewed, and recommends that the Secretary of Commerce approve it as a FIPS.

Version 1 of GOSIP was effective February 1989, and its use is encouraged; it is mandatory in August 1990. Future versions of GOSIP will be mandatory 18 months from the dates of issuance of these future versions.

GOSIP represents a significant resource which may be referenced by both inexperienced and sophisticated OSI users. Products containing OSI functionality referenced in Version 1 of GOSIP are currently available.

3.4 Future of GOSIP

Additions to GOSIP will be developed in conjunction with the GOSIP Advanced Requirements Group, a group of technical experts appointed by Federal agencies. Additions will undergo the same reviews as did the GOSIP FIPS.

As OSI activity progresses in the international standards organizations and the NIST/OSI Workshop, the GOSIP Advanced Requirements Group recognizes this work and develops a schedule for including it in GOSIP. A tentative schedule for including additional OSI functionality is given in the Appendices of the GOSIP FIPS. It is a goal to include new GOSIP functionality as quickly as possible, and to ensure that these inclusions are consistent with current GOSIP technology.

This new functionality includes network security, network management, ISDN (integrated services digital network) capability, connection-oriented network service, dynamic routing, directory services, virtual terminal access capability, and office document architecture and interchange. In addition, steps are underway to enhance the capabilities of applications currently in GOSIP. See section 7 for a detailed description of important new work items.

In the future the OSI functionality referenced by GOSIP will continue to grow to reflect Federal user requirements. Additional versions issued no more than once per year will define completely new OSI functionality, while "building" on the material in previous versions. The work of the international standards organizations and the NIST/OSI Workshop will be fed into the GOSIP creation process. Experience gained by Federal users in GOSIP product assimilation will be input into future GOSIP versions to constantly improve the quality of the document. Requirements of the MAP and TOP groups will also continue to be considered in developing GOSIP.

4.0 GOSIP QUESTIONS AND ANSWERS

Listed below are answers to some of the most commonly asked questions concerning GOSIP.

QUESTION 1: Does GOSIP apply to all procurements of computer network products? If not, to what procurements does it apply?

ANSWER: GOSIP does not apply to the procurement of all computer network products. GOSIP must be cited in solicitations and contracts when the systems and services to be acquired provide functions equivalent to those specified in the GOSIP document.

Version 1 of GOSIP allows users to send and receive electronic mail using the Message Handling Systems (MHS) protocol, and to access and transfer information files using the File Transfer, Access, and Management (FTAM) protocol. In addition, Version 1 provides a reliable end-to-end service between computer systems served by different network technologies. Version 1 of GOSIP is effective in February 1989, and it is mandatory in August 1990; however, Federal agencies are encouraged to reference GOSIP in procurement requests which originate before the GOSIP FIPS is mandatory. For more discussion on GOSIP applicability, see section 5.

QUESTION 2: How can an agency effectively make the transition from its existing systems to the use of GOSIP-compliant products?

ANSWER: There is no single strategy for integrating GOSIP-compliant products with existing systems which will apply to all agencies. The most effective solution will vary with current protocol architecture(s) and the configuration of existing system(s). Some alternatives to consider include the use of dual protocol hosts, application and network layer gateways, and mixed protocol stacks. These alternatives are more fully described in section 9. Current vendors should be consulted in planning a transition strategy. The Department of Defense (DOD) has developed and documented an excellent OSI implementation plan.

QUESTION 3: Will there be future versions of GOSIP? How often will they be issued? Can it be told in advance what is likely to be included in the new versions?

ANSWER: Version 2 of GOSIP will be released in 1989. Version 3 of GOSIP is scheduled for 1990. Subsequent versions will be issued no more frequently than once a year. The appendices of GOSIP give a complete summary of the protocols planned for inclusion in future versions of the document.

QUESTION 4: Who decides what functionality to include in each new version of GOSIP?

ANSWER: The NIST determines and controls the content of each new version of the GOSIP FIPS. The GOSIP Advanced Requirements Group, consisting of Federal agency technical experts, provides assistance and technical input into the specification. The comments of manufacturers, Government agencies, and the public are then solicited. The GOSIP Advanced Requirements Group will consider the technical comments and may recommend revisions to a GOSIP version. Drawing on their technical contributions, the NIST prepares the specification, gets it reviewed, and recommends that the Secretary of Commerce approve a new version as a FIPS.

QUESTION 5: How does the GOSIP Advanced Requirements Group recommend functionality to include in each new version?

ANSWER: The GOSIP Advanced Requirements Group discusses and makes recommendations to the NIST as to which OSI protocols provide services that meet Government needs. The progress made in developing an international standard and implementors agreements for each of these protocols is monitored. Since GOSIP will be referenced by procurement authorities, the GOSIP Advanced Requirements Group also verifies that implementations of these protocols will be available from vendors at the time or soon after the protocol is included in GOSIP. When the GOSIP Advanced Requirements Group completes its recommendations on additions to GOSIP, the NIST incorporates the technical comments into proposed standards which are reviewed by government and industry.

QUESTION 6: An agency is procuring a system which provides directory services. Since directory services is not included in Version 1 of GOSIP, is it true that GOSIP should have no impact on that agency's procurement actions?

ANSWER: The GOSIP appendices should be consulted to determine whether the application functionality that is being procured will be included in a future version of GOSIP. If this functionality is scheduled for inclusion, it would be a mistake not to be forward-looking in a procurement action.

Systems conforming to international standards that provide directory services may be widely available at the time that the system that is being procured is delivered, certainly during the expected lifetime of that system. Contract solicitations should insist that vendor proposals include a plan for making the transition to GOSIP-compliant products.

QUESTION 7 How can it be assured that the GOSIP-compliant products that are purchased have been properly tested for conformance and interoperability?

ANSWER: The National Institute of Standards and Technology plans to issue a GOSIP test policy document specifying procedures for vendors to follow to insure that their GOSIP-compliant products have been properly tested for conformance to the international standard and for interoperability with systems built by other vendors. The test policy will also address the requirements test service providers must meet to receive and maintain Government accreditation. This document will be issued for public review by October 1989 with the goal of issuance of an approved document by August 1990.

The NIST will also provide in 1989 FTAM, MHS and Transport interoperability tests which can be used by Federal agencies in their acceptance tests. In 1990 the NIST will publish procedures for evaluating the performance and functional capabilities of FTAM and MHS implementations. In addition, NIST staff members can work with Federal agency personnel to develop special purpose test procedures.

QUESTION 8: What are the guidelines for requesting a waiver from GOSIP compliance? What are the procedures for requesting such a waiver?

ANSWER: A waiver from the GOSIP Federal Information Processing Standard may be requested when compliance would adversely affect the accomplishment of the mission of a Federal computer system or cause a major adverse financial impact which is not offset by Government-wide savings. For additional waiver guidelines and procedures, consult section 5.3.

QUESTION 9: How can one acquire the knowledge of OSI protocols that is needed in order to make intelligent procurement decisions?

ANSWER: The GOSIP Users' Guide is intended as a first step in providing Federal personnel with the information that they need to make these decisions. In addition, the NIST will hold seminars on GOSIP-related issues from time to time. Commercial organizations will also conduct classes on the OSI architecture and on specific OSI protocols. However, most Federal agency personnel will find that they do not need to be an expert on the technical details of each OSI protocol. In most cases, an understanding of the services offered by the protocols and how the services relate to the mission of their agency is sufficient.

QUESTION 10: What is the relationship of GOSIP to the MAP and TOP specifications?

ANSWER: The MAP/TOP Users Group represents the factory automation and office automation communities. The MAP and TOP documents provide detailed specifications for the OSI protocols that those groups want the vendors to develop to meet their needs. The GOSIP document has a more near-term outlook, since it is intended for use now by Federal procurement authorities. GOSIP provides the information needed to acquire and use the OSI protocols that are or soon will be available from major vendors. Because the developers of GOSIP work closely with the MAP and TOP communities, the OSI protocols in GOSIP are a subset of the MAP and TOP protocols, and MAP and TOP implementations will, in most cases, interoperate with GOSIP-compliant products.

QUESTION 11: If OSI protocols are installed on an agency's computer systems, will communication be possible with all other computers?

ANSWER: No. Open System Interconnection (OSI) protocols define a standard language for communicating data between computer systems, but all computer systems wishing to communicate must speak the same standard language. OSI is analagous to defining a standard natural lauguage (e.g., ESPERANTO) for human-to-human communication. Each speaker then need only know his/her native language and the standard language in order to communicate within the speaker's local community and throughout the world. Thus, if every computer system in the world used OSI protocols, computer systems could, in principle, communicate with all other computers, provided security requirements were met and no OSI dialects existed to hinder interoperability.

The true advantages of adopting GOSIP within a computing environment center on interoperability among computers made by different vendors. The computing environment in Government is increasingly heterogeneous for three reasons: (1) specialists provide superior price-performance in niche markets such as engineering workstations, supercomputers, and disk servers, (2) cheaper computing power allows users to make autonomous buying decisions at lower levels in an organization, only to face later requirements to interconnect, and (3) competitive procurements lead to natural variety among computer suppliers.

In the absence of a data communications standard, the environment created is analogous to a workplace where each worker speaks one, or at most two, of six or seven natural languages. Communication becomes difficult and expensive. Settling upon GOSIP as a standard for data communications within a working environment will enable cost-effective interoperability among a variety of computers.

QUESTION 12: Is GOSIP intended to limit the network technologies available to Government users?

ANSWER: No. GOSIP defines a limited set of standard network interfaces, commonly available as products, for connecting computers to networks. These network interfaces include: (1) packet-switched

network (X.25), (2) carrier sense multiple access with collision detection (IS 8802/3), (3) token bus (IS 8802/4), and (4) token ring (IS 8802/5). While these standard network interfaces are commonly supported by specific network technologies, other arrangements are possible. For example, the IS 8802/3 interface may provide connection to a programmable branch exchange (PBX) using cut-through routing to provide a connectionless data service. The computer system connecting to the 8802/3 interface is unaware that a PBX is the network technology moving the data. The use of the PBX in providing an IS 8802/3 interface is compliant with GOSIP.

GOSIP also permits considerable flexibility with respect to the physical interface. For example, connections to X.25 networks may support RS232 or V.35 depending on speed and distance requirements. As a second example, IS 8802/3 interfaces may be provided using fiber optics techniques, or, technology permitting, twisted-pair telephone wiring.

GOSIP is intended to enable Government users to take advantage of several commonly available vendor products for connecting to networks; however, the true interoperability provided by GOSIP is end-to-end at the Transport Layer with network interconnection provided by the Connectionless Network Protocol (CLNP). The CLNP is used to interconnect a wide variety of standard and nonstandard networks and the Transport protocol is used to provide a reliable end-to-end data path between computers across interconnected networks. Such a reliable end-to-end data path may be used by a wide range of GOSIP application services (e.g., MHS and FTAM) and non-GOSIP applications (e.g., Network File Services).

QUESTION 13: Can ISDN be used with GOSIP?

ANSWER: Yes. Several products are available that act as X.25 terminal adapters for ISDN switches; thus, by using an X.25 interface in a computer and an X.25 terminal adapter, GOSIP permits easy connection to ISDN switches. In a future version of GOSIP, provisions will be made to connect computer devices directly to ISDN switches without requiring an X.25 terminal adapter.

QUESTION 14: Is GOSIP intended to mandate OSI protocols for every Government PC (personal computer)?

ANSWER: No. PCs are small host computers, and GOSIP protocols may be used to provide networking services for PCs; however, several other methods of using PCs in conjunction with GOSIP are possible. For example, GOSIP mail and file transfer services may be made available on minicomputers and/or mainframes accessible to PC users via remote login procedures over serial lines. The placement of GOSIP services within a local systems environment is a technical issue to be decided based on cost and functional requirements, and is beyond the scope of the GOSIP FIPS.

QUESTION 15: If GOSIP protocols are implemented, will computer systems be more vulnerable to unauthorized access?

ANSWER: No. While the interconnection of computers via communication links provides increased opportunity for external intrusion, the use of the GOSIP protocols does not increase the level of vulnerability. Existing standard protocols, such as the TCP/IP suite, are no more or less secure than the newly adopted GOSIP protocols. Work is underway within Government and industry to develop and implement security protocols for use with GOSIP; in fact, a future version of GOSIP will include such security provisions. In the interim, section 6 of the GOSIP FIPS defines a security option for use with the CLNP.

QUESTION 16: Are OSI protocols equivalent to X.25?

ANSWER: No. OSI protocols provide a broad range of network services, historically divided into seven functional layers - the OSI Reference Model. X.25 is a standard defining a protocol for use within the OSI network and link layers. Many other protocols are available to fill out the services in all seven layers of the OSI Reference Model; thus, X.25 is one of the OSI protocols, and is designed to provide specific functionality within several adjacent layers of the OSI Reference Model.

QUESTION 17: Does GOSIP provide programmer-accessible interfaces to network services?

ANSWER: No. GOSIP enables users to purchase products that provide INTEROPERABLE networking services in a multi-vendor environment. For example, GOSIP protocols enable users to send electronic mail to remote users without concern for the type of computer or mail program the receiving user owns. The GOSIP also permits users to transfer files between machines without user concern for incompatibilities in hardware architecture or file system structure. GOSIP enables INTEROPERABILITY between computers.

GOSIP neither mandates nor defines any programmer-accessible interfaces to the network services. Such interfaces may prove useful to achieve SOFTWARE PORTABILITY for programs requiring network services. If a user requires an interface to specific GOSIP-compliant network services, the user must say so in a request for proposal (RFP). If a user desires software portability for programs that use the programmatic interfaces sought in an RFP, the user must not only specify that an interface is required, but also must specify the precise characteristics of the interface. If the interface is not precisely defined, each vendor may provide a different functional interface of the required type. GOSIP IMPLEMENTATION ALONE DOES NOT ENABLE APPLICATION PORTABILITY.

Work is underway to develop standard interfaces to network services. When such work is completed, the results will be included in an NIST-defined Applications Portability Profile. Until that time, users requiring applications portability must precisely define the details of programmer-accessible interfaces to network services. The specification of the interfaces must be included with the RFP.

QUESTION 18: Does GOSIP specify user interfaces to network applications?

ANSWER: No. As described above, GOSIP enables INTEROPERABLE NETWORKING SERVICES between computers made by different manufacturers. In many instances, computer manufacturers add GOSIP services to pre-existing proprietary services without perceptable change to the end user. For example, a user editing and sending mail from a terminal with a proprietary mail package might follow exactly the same set of keyboard actions and witness the same display responses when the GOSIP X.400 (MHS) mail protocol is invoked to relay and deliver the completed message. The user interface is an area where vendors will continue to differentiate their products from those of competitors.

GOSIP neither mandates nor defines any user interfaces to network applications. Such interfaces may prove useful to achieve user portability between computers when network applications are required. If a procuring agency requires a specific user interface to network applications, the details of the interface must be specified. The specification must be included with the RFP. GOSIP ALONE DOES NOT DEFINE ANY PARTICULAR INTERFACE TO NETWORK APPLICATIONS.

QUESTION 19: Are GOSIP-compliant products available?

ANSWER: Yes. Almost every major U.S. computer vendor has announced availability of some GOSIP-compliant products. Transport Layer products were available as early as 1984. CLNP products made a market appearance in 1985. Session Layer products are also available. A variety of local and wide area network products complying with GOSIP are available. The first X.400 electronic mail products appeared in 1986. GOSIP-compliant FTAM products are expected to appear early in 1989. A full range of GOSIP-compliant products, integrated across vendor product lines and including gateways with proprietary offerings, should be available from most major computer vendors when the GOSIP FIPS is mandatory in August 1990. Contact computer vendors for specific product offerings and future plans.

QUESTION 20: Will GOSIP-compliant products cost more than other solutions for data communications?

ANSWER: No. Although vendor pricing strategies are made after considering a large number of business factors, nothing inherent in GOSIP protocols requires compliant products to be more expensive than vendor proprietary offerings; in fact, several factors suggest that long-run pressures will push prices down.

One such factor is implementation variety. GOSIP mandates protocols for interoperable data exchange. Vendors may offer a range of solutions, complying with GOSIP, designed to vary in price. With basic interoperability assured, users may trade price for performance more easily.

A second price suppression factor is alternative sourcing. With GOSIP-compliant products available from a variety of vendors, users may cost-effectively switch to lower-cost vendors without losing interoperability.

A third factor is basic interoperability itself. When a vendor is required to connect equipment with an installed base from a different vendor, use of a GOSIP-compliant solution is likely to be cheaper than implementation of a custom solution.

5.0 GOSIP APPLICABILITY ISSUES

5.1 Introduction

An important decision for Federal agencies is the extent to which GOSIP applies to their particular situations. Given that GOSIP provides economic and planning benefits to users (as explained in sec. 2), it makes sense for every U.S. Government organization to adopt a policy to implement it in future procurements (as stated in sec. 2). Answers will be given in this section to the questions of when and how to apply GOSIP. The OSI protocols specified in GOSIP free users from dependence on a single vendor for new network products and services and promote interoperability across a multi-vendor environment.

Section 2 outlined compelling reasons for an agency to adopt the OSI concept as a strategic initiative; however, each agency is aware of its particular ADP environment and configurations, and each has a unique administrative and political perspective. After reading this section, a user should be able to determine the full extent of GOSIP applicability in a particular environment.

GOSIP should be employed in an agency procurement, planning, and implementation program which involves all ADP and data communications configurations within an agency. The above is true for two reasons: (1) GOSIP provides communications functionality that will meet the requirements of nearly every computer configuration, and (2) GOSIP provides enhanced interoperability.

The approach taken in this section is a deliberate one. First, a broad statement of applicability will be given, emphasizing development of the strategic initiative from section 2. Next, a discussion of waivers and policy decisions will be presented. GOSIP enforcement will be discussed third. After this, specific applicability recommendations are given for Federal agencies. Finally, specific questions will be raised, and answers given, to pertinent concerns and questions users may have regarding GOSIP applicability.

5.2 General GOSIP Applicability

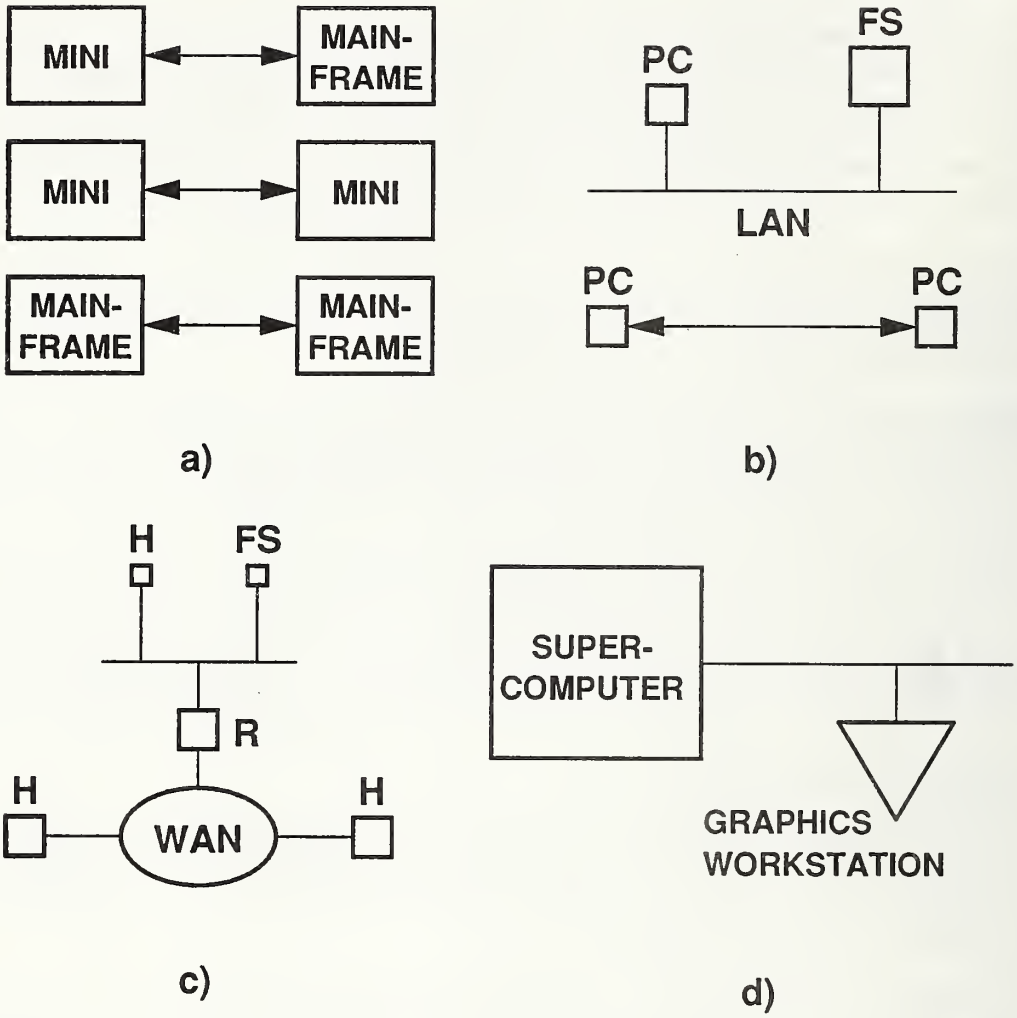
The GOSIP FIPS is effective in February 1989; its use is encouraged, and it is mandatory in August 1990. GOSIP should be applied as part of a broad comprehensive strategic acquisition plan embraced by an agency at the policy level. In light of the benefits of OSI described in section 2, it is anticipated that GOSIP will be applied in most instances where there is a choice.

GOSIP applies to new networking systems which will be procured. Units operating with existing, non-GOSIP networks should add GOSIP-related components into networking systems when such components are available, cost-effective, and efficient for the organization's operation. It is anticipated that with GOSIP all of these conditions will be met.

Since GOSIP deals with communications functionality, and not specific ADP configurations, GOSIP is not bound to any hardware, software, or operating system limitations. This means that GOSIP may apply to all types of systems, in all types of environments. The size of the system is not important in the context of GOSIP; neither is the communications medium used.

There are three general criteria for GOSIP applicability, as follows: (1) the communication must be "computer-to-computer" (that is, between two or more intelligent systems that are able to exchange information), (2) the communicating systems must be autonomous, and (3) the communications functionality must be contained in GOSIP. GOSIP applies to communications between systems, and the use of GOSIP for communications between system components is encouraged where applicable, particularly for distributed systems. Figure 6 gives examples of situations in which GOSIP may be applied.

GOSIP provides two basic capabilities. First, it enables users to request standard applications operating over standard networks. The standard applications supported in Version 1 of GOSIP are File Transfer, Access, and Management (FTAM) [ISO 2-5] and Message Handling Systems (MHS) [CCITT 2-9]; the standard network technologies supported include IS 8802/3 (CSMA/CD) [ISO 6], IS 8802/4 (token bus) [ISO



H = HOST
R = ROUTER
FS = FILE SERVER
PC = PERSONAL COMPUTER
WAN = WIDE AREA NETWORK
LAN = LOCAL AREA NETWORK

FIGURE 6
EXAMPLES OF
GOSIP APPLICABILITY

7], IS 8802/5 (token ring) [ISO 8], and X.25 wide area network [CCITT 1]. For further explanations, see section 7. For example, an MHS user on an 8802/3 network may send a message to an MHS user on an 8802/4 network; these networks may be interconnected by an X.25 network. Second, GOSIP provides a reliable end-to-end service over which users can write their own applications. For example, a nonstandard application to exchange office documents may use the GOSIP end-to-end reliable transfer service, which is provided by OSI layers 1 through 4 (see sec. 7).

The important point is that GOSIP has been deliberately designed to provide a generic set of functionality which may be used in almost any system. Furthermore, it gives a great deal of flexibility to users. Standard networks may be joined to create a large GOSIP-compliant internetwork. In sum, subject to the above constraints, GOSIP generally applies to any ADP environment.

5.3 Waivers and Policy Decisions

A waiver is an exemption from the requirement to purchase GOSIP-compliant products. Once a decision has been made to request a waiver, a procedure must be followed. This subsection will give all information necessary to request a waiver from using GOSIP.

Heads of agencies may waive the requirements of GOSIP in instances where it can be clearly demonstrated that there are significant performance or cost advantages to be gained and when the overall interests of the Federal Government are best served by granting the waiver. Waivers may be requested when functionality critical to an agency mission is not included in GOSIP-compliant products. Waivers may also be requested for special-purpose networks which are not intended to interoperate with other networks, or for products supporting network research.

A waiver request should describe in detail the reasons for the waiver. It should also include a description of the systems being purchased, and a length of time during which the waiver will be in effect. It should be noted that functionality which is not in the current version of GOSIP may be in a future version; thus it is recommended to reconsider the validity of an existing waiver in the future. Adjudication of waiver requests lies entirely within a particular agency. A decision will be made on the merits of the waiver. If a waiver is granted, agencies will be able to purchase alternative (non-OSI) systems for the duration of the waiver. If it is denied, agencies must find a way to translate their requirements into OSI-compliant systems.

A waiver may be requested at any point in the life cycle of a system, and at any relevant point in the procurement cycle. Application may be made by technical or procurement individuals within an agency. It is recommended that a template or standard series of forms be provided by each agency for waiver requests.

For the waiver management process, it is recommended that each agency: (1) appoint a custodian of waiver requests and actions, and (2) develop a procedure for exercising control over the waiver management process. It is further recommended that waiver requests be made in writing, and that actions taken (with reasoning included) be deposited in a single location within each agency. It is advisable that procedures for appeals of waiver decisions be developed within each agency.

It is recommended that a request for a waiver generated within an agency should include:

(a) a description of the existing or planned ADP system for which the waiver is being requested,

(b) a description of the system configuration, identifying those items for which the waiver is being requested, and including a description of planned expansion of the system configuration over its life cycle, and

(c) a justification for the waiver, including a description of the disadvantages that would result through conformance to this standard as compared to the alternative for which the waiver is requested.

The procedures for waivers are given below. Under certain exceptional circumstances, the heads of

Federal departments and agencies may approve waivers to Federal Information Processing Standards (FIPS). The agency head may redelegate such authority only to a senior official designated pursuant to section 3506(b) of Title 44, U.S. Code. Waivers shall be granted only when: (1) compliance with a standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or (2) cause a major adverse financial impact on the operator which is not offset by Government-wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which explains the basis on which the agency head made the required finding(s). A copy of each such decision, with procurement sensitive or classified portions clearly identified, shall be sent to: National Institute of Standards and Technology; ATTN: FIPS Waiver Decisions, Technology Building, Room B-154; Gaithersburg, MD 20899.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register. When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice. A copy of the waiver, any supporting documents, the document approving the waiver, and any supporting and accompanying documents, with such deletions as the agency is authorized and decides to make under 5 U.S.C. Sec. 552(b), shall be part of the procurement documentation and retained by the agency.

It is recommended that all approved waivers be considered interim measures and assigned an expiration date by agency heads (or equivalent officials). It is also recommended that waivered systems be brought into compliance with the present or future GOSIP specification, if possible, and that all waiver requests include information explaining when and how the subject systems will move to the OSI standards. As stated above, all waiver-related documents will be part of the agency procurement documentation and must be retained by the agency.

5.4 GOSIP Enforcement Issues

The Brooks Act (Public Law 89-306) establishes a government-wide program for the development of Federal Information Processing Standards (FIPS) by the NIST. Standards developed by the NIST are approved by the Secretary of Commerce and used by Federal Government agencies. GOSIP has been approved by the Secretary of Commerce as FIPS 146, and enforcement will begin with agency solicitations issued when the GOSIP FIPS is mandatory (August 1990). Enforcement will continue from that point onward, in the manner prescribed by the language of the FIPS, modified by any subsequent insertions or deletions.

Each agency may set up its own enforcement provisions, in addition to those described above. A decision should be made by each agency as to how to enforce GOSIP within that agency.

5.5 Specific GOSIP Applicability Recommendations

Specific recommendations that should be followed when determining whether GOSIP applies to a particular procurement are given below.

(1) Cost savings and GOSIP benefits over the long term should be considered in funding decisions for the current year. With the goal of increased interoperability and functional capability in mind, agencies should not sacrifice future capability for present cost effectiveness.

(2) Multi-vendor interoperability is an important reason for determining GOSIP applicability; however, GOSIP also applies to systems provided by a single vendor.

(3) Agency-specific procedures should be set up as soon as possible to handle waiver management and enforcement issues.

(4) Enforcement of GOSIP will largely be a local agency matter; agencies will have to "police" their own actions.

(5) Due to the benefits of GOSIP, it is expected that waivers will be granted only in exceptional cases.

5.6 Specific Concerns of Agencies

Even after reading section 5.2, questions may arise as to whether an agency's special requirements can be met by GOSIP. Each of the subsections below will address a particular category of user questions, in order for GOSIP applicability to be established.

5.6.1 Functionality

GOSIP should be used by Federal agencies when acquiring computer network products and services that provide equivalent functionality to the protocols defined in the GOSIP document; however, the functionality that is being procured need not be implemented in all hardware components. For example, a Message Handling System could be implemented on a mainframe with personal computers (PCs) providing terminal access using nonstandard software. Figure 7 gives an example of such an implementation.

GOSIP applies to new procurements or major upgrades of networking services specified in the GOSIP document. The question of what constitutes a major upgrade contains subjective elements which must be resolved at the Federal agency level in order to determine whether GOSIP compliance is required. This decision involves "gray" areas in which only general guidance can be given. The addition of a few nodes to a non-GOSIP electronic mail network will not force the agency to retrofit the Message Handling System specified in GOSIP to the entire network; however, a significant expansion of the network would require the agency to procure GOSIP-compliant products and to develop a method of interoperating with the existing mail system if a decision is made not to upgrade that system.

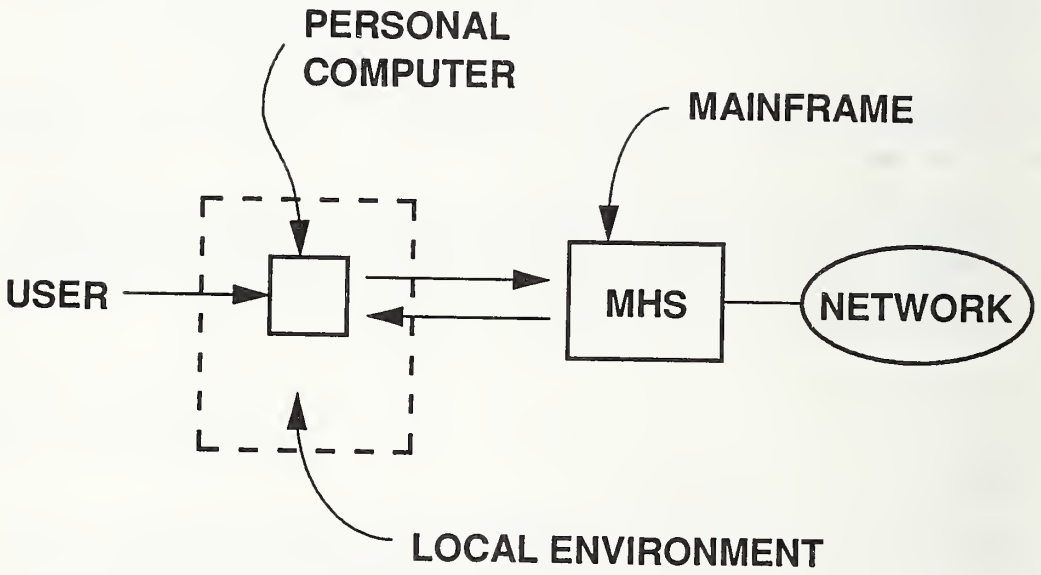
Some Federal agencies may be concerned that the functionality that they require is not in Version 1 of GOSIP. The GOSIP appendices contain a timetable for including additional applications and network services in GOSIP. Procurement authorities should use this information to determine whether it is appropriate to specify GOSIP in current procurements.

EXAMPLE: The Virtual Terminal (VT) application for certain terminal profiles will be in Version 2 of GOSIP, which is scheduled for release in 1989. In 1991, implementations conforming to the OSI international standards will be widely available and procurement of these implementations rather than vendor-specific or proprietary implementations will be mandated by GOSIP. If the VT implementation that is being procured in 1988 is not required until 1991, or if delivery is not expected until that time, then it is wise to specify compliance with the future GOSIP even though it is not yet mandated.

5.6.2 Economic Considerations

A question may be raised as to the cost of GOSIP products versus the cost of other choices. This is particularly relevant in light of total ADP budget constraints and limitations which are imposed on Federal agencies currently. The answer to this concern is that a major benefit of GOSIP is that it is expected to minimize total investment costs through extended life cycles, reduced conversion costs, and increased modularity. Thus, a smaller portion of ADP budgets will be required for purchase and installation of GOSIP technology than for purchase and installation of alternative equipment. Consequently, it is not anticipated that waivers will be requested for economic reasons. In other words, adoption of GOSIP makes good economic sense.

There is no minimum network configuration level specified for GOSIP compliance. Although the OSI



MHS = MESSAGE HANDLING SYSTEM

FIGURE 7
MESSAGE HANDLING SYSTEMS
APPLICATION

protocols referenced in GOSIP are more viable and cost effective when many users and ADP systems are affected, the installation of these protocols is still economical on a per-unit basis even when interoperability is provided only to a few systems.

The initial costs of making the transition to the OSI protocols should not be a reason for GOSIP non compliance. There is a certain amount of overhead, training, and other agency effort required to change to any new technology. The initial cost of this short-term overhead should be greatly outweighed by the long-term cost savings resulting from the purchase and use of these protocols.

5.6.3 Research vs. Operational

A network may be judged as operational or research oriented. Some networks may be aimed at providing research into network function, protocols, or protocol performance. Such networks would not be bound by GOSIP, because it does not make sense to apply a fixed protocol specification to networks investigating possibly varying protocol behavior or performance. Thus, waivers may be granted in this instance. An operational network is one that is oriented primarily toward providing reliable and efficient service to its users given a fixed set of protocols.

The term "network research" should not be confused with the term "research network." Network research involves research into networking technology. This does not imply that waivers are applicable for academic, scientific, or research networks.

It is a recommendation that each agency, using the above definitions and criteria, categorize each network as being operational or involved in network research. Most of the networks in the U.S. Government are operational because they offer basic day-to-day production capability; thus, GOSIP should apply to them.

6.0 GOSIP PROCUREMENT

6.1 Introduction

This section explains how to effectively procure GOSIP products. There is a general description of the procurement process and a discussion of procurement issues as they relate to GOSIP. In section 6.4, specific language will be suggested for users to include in solicitations. In section 6.6, technical evaluation issues, testing issues, and certification issues will be discussed. In section 6.7, vendor enhancements and acquisition strategies will be discussed. Finally will come an enumeration of different kinds of procurement scenarios; since every agency is different, this information is important.

This section will give specific recommendations on most procurement issues relating to GOSIP. For guidance on general procurement issues, readers should refer to their own contracting offices, to the General Services Administration (GSA), or to one of the appropriate references in the References section.

GOSIP is an important document which may be used by both sophisticated and unsophisticated OSI procurement officials. The novice buyer may use the specific procurement language in section 6.4 directly, and the more informed user may modify or add to this language to enable the creation and design of special-purpose applications and configurations in a flexible manner. Additional procurement-related information is given in sections 4.1 through 4.3 in the GOSIP FIPS.

6.2 OSI Procurement Summary

The general stages of an OSI procurement are as follows: (1) the determination by Federal management of a need for ADP equipment, (2) the need for the application user to identify specific requirements, (3) the need to determine whether GOSIP will meet these requirements, (4) the submission of requirements to procurement officials, (5) the determination by procurement officials of the appropriate method to use when creating and structuring the procurement documents, (6) the creation of the solicitation documents, (7) (possibly) an inquiry to prominent vendors as to what can be provided, (8) receipt of bids, (9) evaluation of bids, and (10) presentation of awards. Procurements of GOSIP-related ADP equipment will be bound by any relevant language contained in the FAR (Federal Acquisition Regulations) and/or FIRMR (Federal Information Resource Management Regulations).

In general, there is an order imposed on the above-described steps in the procurement process; in other words, one step must be completed before the next step can begin. The entire process may take a year or more to complete The key step for OSI procurement is the writing of the solicitation document by the user; in particular, the way the requirements are written. This critically affects the outcome of the process. This requirements analysis should be as specific as possible, and be delivered to the procurement officials for formal preparation as procurement documents. It is anticipated that the basic procurement scenario, from the time that the detailed requirements analysis is received by the procurement officials to the actual award of the contract (Steps 4 through 10), will not change in the future because of any conditions pertinent to GOSIP.

It should be emphasized that GOSIP applies to new purchases only; existing contracts and acquisition cycles are not affected. Since the OSI technology is relatively new, it is incumbent upon users to familiarize themselves as quickly as possible with the OSI technology so that informed technical evaluation may be made over the life of an acquisitions process.

Table 1 gives the procurement steps most influenced by GOSIP, in decreasing order of importance, along with some recommended actions.

Table 1 – GOSIP Recommendations

STEP=3, NAME=Determine GOSIP Applicability, ACTION=See section 5

STEP=4, NAME=Submission of Requirements, ACTION=Produce Requirements Analysis

STEP=9, NAME=Evaluation of Bids, ACTION=See sections 6.6 and 7

STEP=7, NAME=Request for Information, ACTION= Draft RFP is Produced

6.3 GOSIP-Related Procurement Recommendations

Described below are aspects of OSI procurement that deserve special consideration by users planning to purchase OSI equipment. Adoption of recommendations stated herein should provide for a smoother OSI procurement process. The recommendations are enumerated below.

(1) In the case of OSI, it is recommended that Federal agencies pursue a competitive procurement strategy (open competition–selection not predetermined) along with a negotiated acquisition, if there are no other policy constraints. This is because the inherent philosophy of OSI is to enable choice among the best networking solutions available. A negotiated acquisition policy applied to selectee(s) will enable users to receive the maximum benefit in services provided.

(2) Agency officials should consider both present and future GOSIP functionality when making long-term procurement decisions.

(3) A draft purchase request is a preparatory document designed to elicit vendor comment; this is in advance of a formal purchase request. It is recommended that for OSI products, a draft RFP (request for proposals) be created. This is because it is important to determine what the vendors are able to provide; also, the OSI technology will be emerging in a series of steps or stages, and what can be provided next year may not be available this year.

(4) It is recommended that a clear, concise statement of work be developed for every planned OSI acquisition. This will reduce the number of questions asked of a solicitor by the vendors after an RFP is issued, and shorten the effective evaluation time.

(5) For OSI, it is likely that smaller vendors will "join forces" to submit bids in competition with larger vendors. This will enable all OSI vendors to compete in the market, and give the user many alternatives from which to choose. Users should be aware of this in their procurement planning.

(6) Since OSI is a new technology, agencies should consult with several vendors to determine a fair price; however, awards are expected to be made on technical merit as well as price.

(7) For OSI procurements, compliance to specified requirements must be accurately determined. Contractors responding to bids should be required to provide test certification from an authoritative source, or perform testing to demonstrate full compliance to the specified requirements. A GOSIP testing policy is under development by the NIST.

(8) A list of customers who are using the OSI product should be required, if possible. The contractor should provide a plan for operational demonstration in the proposal. This plan shall delineate the methods by which the contractor intends to demonstrate to a U.S. agency how the proposed OSI product satisfies the stated OSI requirements. The agency will review this plan and ensure all requirements are tested and met.

(9) An acquisition plan should be developed for every OSI system under consideration by an agency for the next 10 years. Such a plan should include provisions for demonstration of source competence.

(10) OSI products might be available from standard GSA schedules, both independently and bundled with hardware. Even though the numbers of such OSI products will be small in the near future, Federal users should investigate the GSA schedule option.

6.4 Particular "Contract Language" for RFPs

In previous subsections the general procurement considerations for GOSIP were given, and recommendations were made on issues pertinent to OSI. However, this is only meaningful if the user knows exactly what language to insert at the appropriate point in a solicitation document; recommendations will be given here, as well as guidelines for protocol selection and service interface definition. For more detailed guidance on these technical matters, the reader should refer to section 7 and to the Appendices.

It should be emphasized that (1) GOSIP specifies COMMUNICATIONS technology, and (2) GOSIP specifies functional requirements, not specific technical requirements in terms of particular ADP configurations. Thus GOSIP deals with communications capability ONLY; all other ADP concerns are outside the scope of GOSIP. Also, GOSIP provides (1) reliable end system-to-end system service over different network technologies, and (2) applications that conform to international standards that use this reliable end-to-end service. Thus users are able to write special purpose applications conforming to (1) and (2) above.

EXAMPLE: An agency stores inventory data on magnetic tapes which are hand-carried from building to building. It is desired to replace this "system" by one using local-area network technology. GOSIP is certainly a candidate for consideration in this upgrade.

6.4.1 Determining Requirements

In general, the user should first determine what the application requirements are, and whether those requirements may be satisfied by GOSIP applications (initially file transfer and electronic mail). There is a set of generic applications which are used in most Federal agencies. These include: basic file transfer, electronic mail, remote login, remote database access, electronic data interchange, and office document architecture and interchange. The user, in preparing a requirements specification for later solicitation, should examine the goals of the particular application or program, and look at the mechanisms or services by which these goals will be achieved. In other words, a user must determine functional requirements for the application. If those functional requirements can be met by any of the GOSIP protocols, then compliance with GOSIP must be specified in future solicitations.

Factors in the above determination will be the length of the procurement process and the timetable for availablity of additional OSI functionality. It is important to remember that additional functionality reflecting user requirements will be added to future GOSIP versions.

It is possible for the user to have particular requirements for applications. The user needs to determine whether OSI products are consistent with and can support these requirements.

If this determination can be made, then OSI products must be specified in requests for proposals issued when the GOSIP FIPS is mandatory in August 1990. If any other condition exists (e.g., the required functionality is not GOSIP-related, or there is a special architectural requirement), then a waiver may be requested. If granted, the user may specify alternative (non-OSI) solutions in solicitations.

In addition to application functional requirements, there are network technology requirements that must be considered by a user in a requirements analysis. As shown in figure 3.1 of the GOSIP FIPS, there are four alternatives; any of these is acceptable in a solicitation. Any of the GOSIP applications may reside "over" any of the network technologies. Similarly, the user must determine functional requirements for end-to-end transmission, and determine if the GOSIP-compliant technologies satisfy these requirements. For an existing system, it must be determined if specialized network technologies currently in use are able to apply GOSIP technologies to satisfy functional requirements. If requirements can be satisfied, then one of the GOSIP network technologies must be chosen in a solicitation. If nonstandard network technologies are required,

GOSIP may still prove useful for network interconnection, end-to-end transport, and applications. If any other condition exists, a waiver may be requestsd.

EXAMPLE: An agency has dissimilar Ethernets which use different physical media and are located in Florida, California, and Louisiana. These LANs are connected to mainframes which communicate using proprietary protocols over dedicated leased lines. It is desired to standardize LANs and upgrade to a single wide area network protocol (to save money). The GOSIP network technologies should be used.

6.4.2 Specific Language

The procurement language below can be included directly in solicitations for purchasing the appropriate OSI products. The knowledgeable OSI user may modify or add to this language to suit individual requirements.

FTAM LANGUAGE

If a requirement exists for limited file transfer and management capability (such as that supplied by a print server), include language as follows:

"The product must conform to sections 4.2.5, 4.2.6, 4.2.7.1, and 4.2.7.2 of the Version 1 Technical Specification portion of FIPS 146. Specifically, FTAM functionality must be in accordance with 4.2.7.2, ACSE functionality must be in accordance with 4.2.7.1, Presentation Layer functionality must be in accordance with 4.2.6, and Session Layer functionality must conform to 4.2.5. For FTAM, Implementation Profiles T1 and M1 must be supported as stated in 4.2.7.2. The product must be able to act in the FTAM role(s) of X."

In the above language "X" represents one or more of the allowable combinations of "initiator-sender," "initiator-receiver," "responder-sender," and "responder-receiver," as described in section 6.17.1 of the NIST Workshop Agreements [NIST 1]. See section 7.4.3 for more information.

For greater file transfer, access, and management capabilities (such as those provided by a file server), use the language above with the replacement of "[T1 and M1]" by "[T2, M1, and A1]."

For further detail on above-mentioned capabilities, consult the NIST Workshop Agreements [NIST 1]. The coordination with vendors should be done before inserting the language in the paragraph above, because some early FTAM implementations may not have these enhanced capabilities. See section 6.5.1 of this Guide for additional procurement considerations.

MHS LANGUAGE

The terms "MHS" (for Message Handling Systems) and "X.400" are frequently used to refer to an application which allows users to send and receive messages over a store-and-forward message transfer system. If a requirement exists for electronic mail capability, include language as follows:

"The product must conform to sections 4.2.5 and 4.2.7.3 of the Version 1 Technical Specification portion of FIPS 146. Specifically, MHS functionality must be in accordance with 4.2.7.3, and Session Layer functionality must be in accordance with 4.2.5."

The solicitation must state whether Transport Class 0 is required, in addition to Transport Class 4 (see sec. 4.2.7.3 of the GOSIP FIPS). See section 6.5.2 of this Guide for additional procurement considerations. For more information on these CCITT Recommendations refer to section 7.

NETWORK TECHNOLOGY LANGUAGE

If a requirement exists to specify a local area network with a CSMA/CD architecture, include language as follows:

"The product must conform to sections 4.2.1, 4.2.2 (as modified below), 4.2.3, and 4.2.4 of the Version 1 Technical Specification portion of FIPS 146. The modification to 4.2.2 consists of adding a sentence as follows: "ISO 8802/3 shall be selected." In addition, intermediate systems must conform to section 4.3."

If a requirement exists for a local area network with a control access bus architecture, use the same language as above except replace "IS 8802/3" with "IS 8802/4." If a requirement exists for a local area network with a control access ring architecture, use the same language as above except replace "IS 8802/3" by "IS 8802/5."

If a requirement exists for a network technology using wide area X.25 network facilities, specify language as follows:

"The product must conform to sections 4.2.1, 4.2.2, 4.2.3, and 4.2.4 of the Version 1 Technical Specification portion of FIPS 146. In addition, intermediate systems must conform to section 4.3."

If a requirement exists to integrate multiple network technologies into a GOSIP-compliant internetwork, specify language as follows:

"The product must integrate multiple network technologies (as described in 4.2.1 and 4.2.2 of the Version 1 Technical Specification portion of FIPS 146), in a manner prescribed by 4.2.3 of the above reference."

See section 6.5.3 of this Guide for additional procurement considerations.

6.5 Optional Procurement Considerations

THE LANGUAGE IN SECTION 6.4.2 IS SUFFICIENT FOR GENERAL OSI PROCUREMENT. SPECIFICATION OF OPTIONS DESCRIBED BELOW REQUIRES TECHNICAL KNOWLEDGE.

AGENCY TECHNICAL OFFICIALS SHOULD BE PROPERLY INFORMED ON THESE MATTERS BEFORE THIS MATERIAL IS INCLUDED IN SOLICITATIONS. CONSULT SECTION 7 FOR ADDITIONAL INFORMATION.

This section will list special options regarding procurement of file transfer, access, and management (FTAM) products and MHS products. Service interface definitions, network technologies, Presentation, Session, gateways and some future procurement considerations are also mentioned. Products are expected to provide a variety of optional services and features. Appropriate language extensions will be given for each feature.

6.5.1 FTAM (File Transfer, Access, and Management)

For FTAM there are the two broad classes of products desribed in section 6.4.2; one class offers limited file transfer and file management capability and the other offers greater file transfer, file access, and file management capability. It is expected that there will be a variety of other options provided in FTAM products. Some of this functionality may not be available in the near future, but it will be made available eventually in response to user demand.

Several classes of options may be considered, and may be specified independently of one another. Such options describe additional capability to that offered in section 6.4.2. The categories are given below.

(1) Full file transfer allows reading to and writing from indexed files. To reference this, add a sentence to the full quoted (") paragraph in the "FTAM LANGUAGE" part of section 6.4.2 as follows: "Implementation Profile T3 as defined in the NIST Workshop Agreements must be supported." See section 6.19.3 of Version 1 of the NIST Workshop Agreements [NIST 1] for more information on T3.

(2) Full file access allows locating and erasing within indexed files. To reference this, add a sentence to the full quoted (") paragraph in the "FTAM LANGUAGE" part of section 6.4.2 the following: "Implementation

Profile A2 as defined in the NIST Workshop Agreements must be supported." See section 6.19.5 of Version 1 of the NIST Workshop Agreements [NIST 1] for more information on A2.

(3) File storage capability allows retrieval of complete information on file storage properties. To reference this, add the following sentence to the full quoted (") paragraph in the "FTAM LANGUAGE" part of section 6.4.2: "The storage group of FTAM attributes, as defined in ISO 8571-2 [ISO 3], should also be supported."

(4) File security capability (for banking systems) allows the retrieval of file security properties. To reference this, add the following sentence to the full quoted (") paragraph in the "FTAM LANGUAGE" part of section 6.4.2: "The security group of FTAM attributes, as defined in ISO 8571-2 [ISO 3], should also be supported."

(5) File directory capability is used for sending and receiving file directory information. To reference this, add the following sentence to the full quoted (") paragraph in the "FTAM LANGUAGE" part of section 6.4.2: "The document type NBS-9 as defined in the NIST Workshop Agreements must be supported."

6.5.2 Message Handling System (MHS) Options

In terms of MHS systems, the major components of a Message Handling System implementation are the Message Transfer Agent (MTA) and the co-operating User Agents (UAs). In addition to interacting with the Message Transfer System, the User Agents have many local functions which are outside the scope of international standardization, but not outside the scope of legitimate procurement concerns. These services include assisting the originator in creating and editing the message and in storing and presenting a delivered message to the recipient. These services will be provided in all User Agents but any specific user requirements for these non-standardized services should be specified in the procurement request.

Agencies that have the requirement to write their own nonstandard User Agents should specify a programmer-accessible interface between the User Agent and the Message Transfer System. If there is a requirement for a special-purpose User Agent, a sentence should be added to the MHS description in Section 6.4.2 as: "The User Agent shall provide the following capabilities:...," and then have these capabilities listed.

User requirements for the generation of optional Interpersonal User Agent elements should be specified. See section 7.4.2 and Appendix A for details. If it is desired to communicate over public messaging domains via public data networks, and an explicit service is required, add a sentence: "The product must be capable of communicating with CCITT-based public messaging systems."

6.5.3 Network Technology Options

The following applies to additions to the network technology language in section 6.4.2. The network technology choices are dependent upon the physical transmission capabilities employed. If compatibility with twisted-pair technology is required, then add the following sentence: "The Physical Layer must be compatible with twisted-pair media, as defined in the appropriate ISO 8802 standard." If coaxial cable is required, then add the following sentence: "The Physical Layer must be compatible with coaxial cable technology, as defined in the appropriate ISO 8802 standard." If fiber optic compatibility is required, then add the following sentence: "The Physical Layer must be compatible with fiber optics, as defined in the appropriate ISO 8802 standard." If any other physical medium is required, add the sentence: "The OSI product must support the following physical medium:..., as specified in ...."

The transmission technique choices are: (1) for 8802/3 based systems, 10 BASE 5 or 10 BROAD 36, and (2) for 8802/4 based systems, 10 Mbps (broadband) or 5 Mbps (carrierband) (see NIST Workshop Agreements [NIST 1]). For (1) choosing 10 BASE 5 add: "The 10 BASE 5 CSMA/CD technology shall be supported. as defined in NIST Workshop Agreements [NIST 1]." For (1) choosing 10 BROAD 36 (for communication with 8802/4 broadband systems) add "The CSMA/CD 10 BROAD 36 technology will be supported, as defined in NIST Workshop Agreements [NIST 1]."

For (2) above, if choosing 10 Mbps broadband, add "For 8802/4 systems, the 10 Mbps broadband technology will be supported, as defined in NIST Workshop Agreements [NIST 1]." In choosing 5 Mbps baseband, add "For 8802/4 systems, the 5 Mbps baseband technology will be supported, as defined in NIST Workshop Agreements [NIST 1]."

6.5.4 Service Interface Choices

Users should state their functional and operational requirements in solicitations and leave the method of implementing those requirements to the vendors. Certain user requirements will cause vendors to supply a programmable service interface. These service interfaces constitute a "boundary" through which information flows from one OSI layer to an adjacent layer. Some common points at which programmable service interfaces may be provided by vendors are: (1) an Application Protocol (e.g., FTAM) - ACSE (Association Control Service Element) interface, (2) a Session-Transport interface, and (3) a UA-MTA interface.

Defining specific interfaces for purposes of portability is a task beyond the resources of most users. Users with such requirements should support defining standard interfaces to POSIX network services.

6.5.5 Gateway Considerations

In migrating to an OSI environment from the current ADP environment, it may be necessary for technical or procedural reasons to explicitly require a gateway in a solicitation. Such a gateway would convert information in a vendor-specific or proprietary protocol to equivalent information in the OSI protocol and vice versa. If this action is necessary, add a sentence to any of the paragraphs in section 6.4 as: "The OSI gateway must be able to completely and effectively convert between [A and B], and the vendor must document impacts on services and protocols provided by the gateway." Here A and B are specific protocols.

Quite often, vendors will provide gateway capability as described above as a largely transparent "value-added" service. Users should discuss such possibilities with vendors as part of the acquisition process.

6.5.6 Presentation and Session

The NIST Workshop Agreements require that the Presentation kernel functional unit be supported. This supports the services required to establish a Presentation connection, transfer normal data, and release a Presentation connection. The Application Layer protocols determine the Session layer functional units needed for their support. For an explanation of the above-mentioned capabilities, refer to section 7.

6.5.7 Future Considerations

Additional OSI protocols and services are expected to be available within the next few years. Specific procurement language will be given when these protocols and services are included in a future version of the GOSIP FIPS. For additional information on this ongoing work, refer to section 7 of this Guide and to the appendices to the GOSIP FIPS.

6.6 Evaluation Process for Procurement

Technical details necessary for proper evaluation will be described in section 7 and Appendix A of this document. Federal applications users should solicit appropriate technical individuals to analyze their requirements. It is extremely important that evaluation responsibilities be assigned only to individuals that have an understanding of system specifications, system requirements, acquisition regulations, and contract administration.

The OSI evaluation process involves: (1) interpreting technical information contained in product announcements, (2) determining a process for ranking candidates, (3) making a selection, and (4) providing complete documentation to those who were not selected. All of these steps must be completed for proper OSI evaluation. Step 1 should be embodied in an acquisition plan or statement of work, and should be devel-

oped by administrators, in conjunction with technical advice. Step 2 should be accomplished by reading the GOSIP Version 1 Technical Specification, section 7 of this Guide, and appendices, and be done by technical experts. In Step 3, OSI requirements may be classified as critical (mandatory) or desirable (optional). Each agency should design an appropriate weighting scheme for technical merit factors, cost factors, and planning factors. Step 4 is a natural consequence of Step 3. Unsuccessful bidders should be provided with (if possible): name of successful bidder, complete list of bidders, and rationale for nonselection.

In the GOSIP FIPS, the term "acquisition authority" embodies the planning, procurement, and technical evaluation authorities. All of these functions may be assigned to one individual, or each function may be assigned to a separate individual.

OSI products will be evaluated on the basis of (1) conformance, (2) interoperability, and (3) performance; these are described briefly in the GOSIP FIPS. The NIST is developing a conformance and interoperability test policy for GOSIP products. The goal of the policy is to provide the Government buyer with the utmost assurance that offered vendor products conform to the GOSIP requirements and interoperate among themselves. The formal policy will be subject to open review and may change. The GOSIP testing policy will be published in a separate document from this GOSIP Users' Guide.

The contracting officer's review of nontechnical OSI factors will generally be divided into two phases: (1) a review of the business aspects of the bid or offer, and (2) a business review of the contractor's operations and qualifications. It is recommended that the requiring activity not be made aware of the total prices proposed. This is to ensure that technical evaluations are based solely on technical factors, and are not influenced by price.

The negotiation method should be used with all large purchases; for small purchases a straight "low bid" approach may be taken; this is particularly true for "generic" OSI technology. Furthermore, since OSI products represent an early phase development activity, it is recommended that Federal agencies negotiate with the most highly-qualified vendors to obtain the maximum OSI functionality desired, even if the cost is not minimal. Selection should be based on functionality supplied, not cost alone.

An extensive set of benchmark tests may be required in a RFP; these tests should span the entire range of capabilities required by a system. Demonstrations should be mandated for each vendor. These benchmarks should be fair and open and should not bias one vendor in favor of another. Technical experts at each agency will identify critical and noncritical OSI product capabilities to be tested.

For proper and complete evaluation of GOSIP products, since OSI technology is new, it is recommended that a review of at least 3 months be undertaken for all commercially available OSI products. This recommendation is waived when: (1) minor OSI components are being considered, and (2) in the future, when bids are received from contractors who would have previously produced identical OSI products for the Government.

6.6.1 Conformance Testing

Conformance testing verifies that a protocol implementation performs as the standard specifies. Most conformance test scenarios concentrate on single layer testing. One layer of the OSI protocol stack is tested at a time using the services of the lower layers which have been tested previously and are assumed to be correct.

Conformance testing alone will not ensure that an OSI protocol suite will work correctly. No conformance test system can ensure that all errors in a protocol implementation will be detected. In addition, single layer conformance testing is not always possible, because some vendors merge the functionality of two or more layers in a protocol implementation.

Agencies may request, on an interim basis, statements of completion of conformance testing from vendors or testing service centers. These statements should specify the functions tested and the results. Once the

NIST GOSIP test policy is established, this interim guidance will be superseded.

6.6.2 Interoperability Testing

Interoperability testing simulates the "real-life" conditions under which the vendor's product will be seen. Since vendors of OSI products are building implementations to operate with implementations developed by other vendors, it is in both the customer's and vendor's interest to duplicate as closely as possible the environment in which the product will be used before product acceptance is completed. Interim guidance, pending a completed GOSIP test policy, is given below.

Agencies may specify the products to be tested, the tests to be passed, and the criteria for passing the tests. Alternatively, agencies could request statements of completion of interoperability tests which include a list of vendors tested with and specific functions tested. Since all testing adds to the total cost, agencies are discouraged from specifying special interoperability testing that is not required. If agencies require testing of additional functionality, they should require that the vendor perform additional interoperability tests, as a part of the acceptance testing process. Each agency should develop expertise concerning functional capabilities tested and the meaning of any test results. If necessary, there should be additional testing "in house." Vendors should provide the results of a standard set of interoperability tests on their products prior to bidding, if possible.

6.6.3 Performance Testing

Federal agencies may compare performance data produced by research organizations with agency requirements. The NIST may provide advice on realistic performance requirements given certain technological considerations. In addition, users need to determine the performance requirements pertinent to their particular situation. The NIST is developing performance metrics and benchmarks for GOSIP.

6.6.4 OSI Testing Information

Until a GOSIP test policy is developed, Federal agencies are encouraged to consult OSI testing centers to get lists of products. Federal agencies are also encouraged to watch for press releases and public announcements from vendors.

There are several places to go in the United States for product testing information, including the Corporation for Open Systems (COS) and the Industrial Technology Institute (ITI). Vendors may also create their own test centers. Lists of conformant products, according to type and level of conformance, will be available from the testing centers. The NIST is developing a policy to address identifying, evaluating, and certifying tests, test methods, and test services.

6.6.5 Recommended Interim Testing Policy

Evidence of conformance to the standards and of interoperability between specific configurations should be mandated. Performance tests may be important or unnecessary, depending on a particular agency's requirements. It is recommended that successful completion of conformance and interoperability tests be considered a critical requirement. Close cooperation should be maintained with the vendor community in the testing process.

EXAMPLE: Agency X, to save money, allows evidence of conformance and interoperability from Vendor X and from Vendor Y to be supplied by vendors. Performance tests are scheduled on site, since this agency has specific performance requirements. The on site performance tests serve to demonstrate interoperability, if the proper configurations are used.

6.7 Vendor Enhancements and Acquisition Strategies

If agencies have particular needs that may not be satisfied by current OSI standard products, then they

may request and respond favorably to enhancements containing these nonstandard or interim services. As a part of a vendor response, a transition plan should be included indicating how these nonstandard services will evolve to standard OSI solutions in the future.

Several examples are apparent, in the form of directory service enhancements and network management solutions. In either case, vendors may offer interim solutions as enhancements to OSI products, in the absence of standards supporting these capabilities. Interim specifications (i.e., MAP/TOP) may be proposed as a short-term solution. Users may wish to accept these options, and require that the vendor propose a transition path to the standard OSI solutions when they become available in products.

Another example is that of security enhancements to OSI products. Many users have security needs that must be added as options to existing OSI products. Comprehensive security standards are not available currently. Users may accept interim security solutions, if needs exist. These solutions should be moved to OSI solutions in the future, and it is recommended that vendors provide a plan or specific commitment for such a transition.

6.8 Specific Examples of Procurement

Each agency will find itself with different procurement concerns, because the characteristics of each agency are different. Each agency has its own set of system life cycle and configuration decisions to make; these will be more fully explored in section 9. This fact will affect the procurement decisions that must be made. Some general procurement-related scenarios may be defined. It is likely that an agency will find itself in one of these procurement scenarios.

The first procurement scenario is one in which all procurement efforts are contracted out (and then given to subcontractors). In this situation the Federal official should interact frequently with non-Federal contractors to ensure that the wishes of the Federal officials are being met in the contracting process. This includes specifying when and how benchmarking tests are to be run, specifying application performance requirements, and monitoring the life cycle of the contract, including when and how the contract money is to be spent. This is particularly critical in the area of system upgrades.

A second procurement scenario is one where there are a number of large pre-existing proprietary networks that will be extant for the next few years. The stated purpose of OSI products will be to interconnect existing networks and maintain existing applications. A procurement strategy here would be to specify OSI gateways, routers, or possibly dual protocol suites. For more information on gateways, dual suites, and routers, consult section 9.

A third procurement scenario is one where system upgrades occur; that is, additional OSI capability will be developed, and major additional OSI hardware and software purchases will be contemplated. However, this expansion is entirely under the control of one central authority. As system life cycles expire, replacement will occur with OSI technology. The strategy here is to develop at the outset a comprehensive long-term acquisition plan which will describe progress at a steady pace toward a complete OSI environment at some specified time in the future. Key dates should be identified when specified "levels" of OSI functionality should be achieved. Gateways may be procured as part of a transition strategy.

The fourth procurement scenario is similar to the third, but in this case, there are many different centers of administrative and technical control. Different components of an agency may be at different stages in OSI evolution, and close cooperation must be maintained with the regional centers to move towards an integrated OSI environment as soon as possible. The procurement strategy here is for each center of authority to develop an acquisition plan for its environment, and for there to be a series of meetings to coordinate progress towards OSI. Each center of control should not be "bound" or "restricted" by the nature of acquisition strategies at other centers. There should be an effort to embody all of the possible procurement strategies in a comprehensive transition plan for the entire agency.

An agency should determine which of the above scenarios applies, and take the indicated actions. Table 2 summarizes the example generic procurement scenarios depicted, and the appropriate actions in each case.

Table 2 – Procurement Scenarios

CATEGORY=Contracted Out, STRATEGY=Contractor Monitoring

CATEGORY=Connecting Networks, STRATEGY=OSI Gateways and Dual Suites

CATEGORY=System Upgrade (Centralized), STRATEGY=Centralized Acquisition Plan

CATEGORY=System Upgrade (Distributed), STRATEGY=Distributed Acquisition Plans

CATEGORY=System Upgrade (Distributed), STRATEGY=Overall Transition Strategy

7.0 TECHNICAL ISSUES

7.1 Introduction

This section provides supporting technical documentation necessary to perform proper evaluation of vendor proposals as described in the previous section. The user will need to understand this material in order to interpret product announcements. Upon completing this section a user should have a greater awareness of the technical capabilities of OSI products. The Federal technical specialist evaluating GOSIP products must be aware of the technical issues to be considered at the time the evaluation is made. The technical advisor after completing this section should have a greater understanding of OSI concepts.

This section gives (1) a summary of the OSI Model, (2) a synopsis of technical considerations in three areas (protocol, service interface, performance), (3) guidelines for evaluating information in product announcements, and (4) some examples of OSI information flow. For an evaluation of technical considerations, readers should refer to subsections 7.3 and 7.4. For an interpretation of product announcement information, readers should refer to subsection 7.5. For examples of OSI scenarios, readers should refer to section 7.6. Descriptions of future work important to GOSIP are given in section 7.7. For additional tutorial material, refer to Appendix A, and for the actual standards references themselves, refer to Appendix B.

7.2 OSI Reference Model Summary

The OSI standards were developed to allow computer systems built by different vendors to exchange data. Even though these computer systems have different operating systems and vary in how data is processed internally, as long as the information that passes between the processors conforms to the OSI international standards, it can be interpreted upon receipt and communication is possible.

The first step in OSI standards development was the creation of an OSI Reference Model [ISO 1]. This model was developed by the International Standards Organization (ISO) and is divided into seven layers; each layer provides a well-defined function necessary for the effective transmission of data. Each of these layers provides a service to the layer above by carrying on a conversation with the same layer on another processor. The rules and conventions of that conversation are called a protocol. At each layer N, there is an N-layer protocol. The information that is passed between a layer on one processor and the corresponding layer (or peer entity) on another processor is called a protocol data unit.

Service primitives are special messages which define the services that the lower layer provides to the upper layer. The details of how the services are implemented are transparent to the upper layer. Communication between layers is via a service access point, or a special location through which this communication passes. Service request and service response information pass between adjacent layers at the service access point.

Brief descriptions of the services provided by each of the seven layers of the model are given in the GOSIP FIPS. The important principles are that (1) each layer performs a unique, generic, well-defined function, and (2) layer boundaries are designed so that the amount of information flowing between any two adjacent layers is minimized. A particular layer has to provide a sufficient number of services to the layer immediately above for that layer immediately above to properly perform its functions. The ISO international standards (ISs) and CCITT (Consultative Committee for International Telegraph and Telephone) recommendations are based upon the same Reference Model shown in figure 8.

The functions of each of the protocol layers will be explained later in this section. The protocols can be connection-oriented or connectionless. In connection-oriented protocols, a user must set up a virtual "dedicated" connection, which is valid for the life of the communications activity, and disappears when the communications activity disappears. The converse of this is connectionless activity, whereby the user does not set up a virtual connection but communicates by transmitting individual "pieces" of information. An example of the former is a telephone conversation; an example of the latter is message delivery by the postal service.

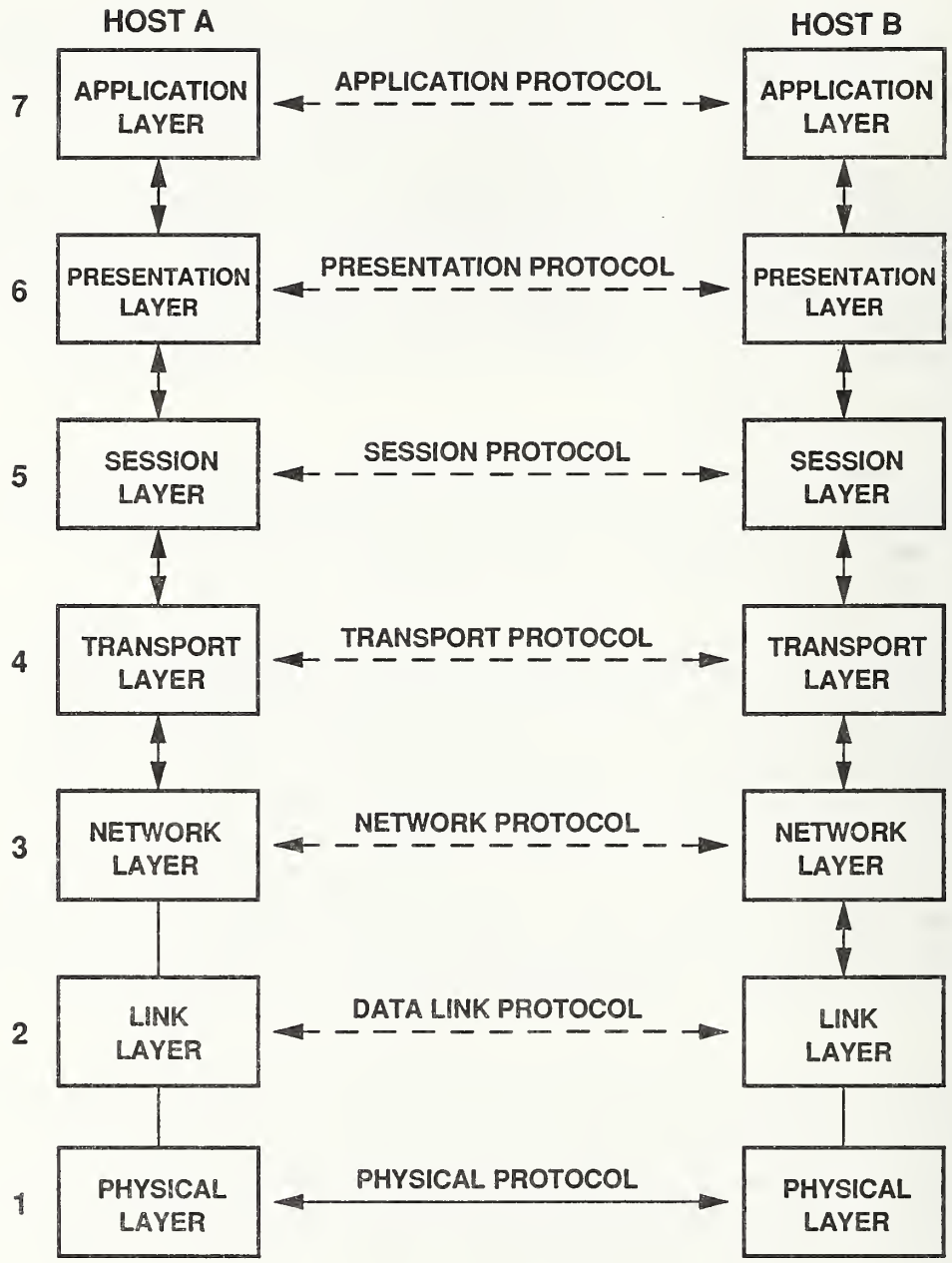


FIGURE 8
ISO REFERENCE MODEL FOR OSI

The relationship of the layers in the OSI model has been compared to a "wine glass." A number of user applications are defined (top of the glass). Each of these may have slightly different means of support from the functional layers (sides of the glass). All applications have reliable end-to-end service provided via the Transport Layer and Connectionless Network Protocol (stem of the glass). This is the "glue" that holds the top and bottom together. At the bottom are the various network technologies (base of the glass). Figure 9 illustrates this.

7.3 Protocol Considerations

Based on the general information given above, the functional capabilities of each of the protocols referenced in the GOSIP FIPS are described below. The discussion includes a description of capabilities provided by the protocol (to assist the user) and, where applicable, options as to how the protocol might be implemented. It should be a vendor decision as to how to implement OSI protocols, but users should have a general knowledge of possibilities so that they can evaluate vendor offerings and can make special requests, if necessary.

7.3.1 Association Control Service Element (ACSE) Protocol

ACSEs provide common services that are expected by a number of applications; it is more efficient to incorporate these services into a common protocol than to reproduce them in every application. The ACSE protocol performs essential services for the application, such as connection establishment, connection release, and error notification. An everyday example is a telephone conversation, where a secretary establishes a telephone connection for a manager.

7.3.2 FTAM Protocol

"FTAM" in GOSIP describes the File Transfer, Access, and Management (FTAM) Standard. This standard provides a means of communicating about groups of related information, i.e., files. A user can move files, interrogate the properties of files, and manipulate files on a variety of different systems, without knowledge of the characteristics of any particular file system. This is accomplished by means of a common communications model and language, as described in the standard.

Services of FTAM provided to the applications user are: (1) the ability to communicate about files without specific knowledge of the other system's file characteristics, (2) the ability to express exactly what the user requires, and (3) the ability to include detailed transfer, access and management mechanisms.

FTAM describes a two-party interaction between an initiator and a responder that reacts to the initiator's requests in a passive role. Steps in a typical FTAM activity are to: (1) establish an FTAM association with a recipient, (2) select a file, (3) modify the properties of that file, (4) open that file, and (5) perform data transfer on that file. FTAM allows one to access and transfer an arbitrary number of different file types, and allows detailed (record-level) access to any one type where appropriate. For more details on FTAM, consult Appendix A.

7.3.3 Message Handling Systems

The Message Handling Systems application is based on the CCITT X.400 Series of Recommendations. These Recommendations specify a store-and-forward Message Transfer System consisting of individual Message Transfer Agents which cooperate to deliver a message from Interpersonal User Agents serving an originator to Interpersonal User Agents serving one or more recipients.

An analogy is that of a user writing a letter (message), inserting it into an envelope, and delivering it to a post office. Envelope and contents are routed to a destination post office via intermediate post offices (possibly); once at the destination, that post office delivers the letter to the recipient's home. The destination User Agent is the recipient's mailbox; the post offices are Message Transfer Agents.

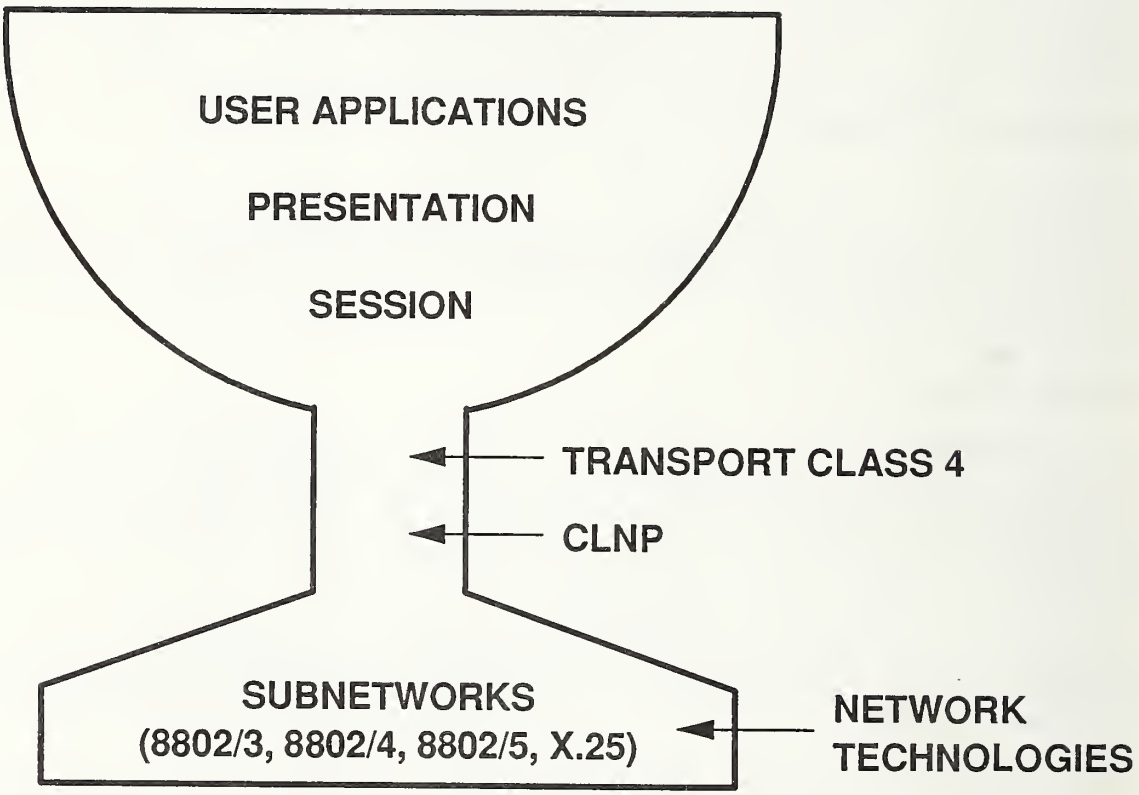


FIGURE 9
OSI "WINE GLASS" EXAMPLE

The Message Transfer System, like the post office, provides special services such as delivery and non-delivery notifications, priority delivery, and deferred delivery. The User Agents which submit messages to and receive messages from the Message Transfer System can be under the same management as the Message Transfer System, or they can be under separate management.

A message consists of an envelope and contents. The envelope contains address information, and the contents may contain different encoded information types. In sum, the MHS provides an efficient means of transmitting messages from an originator to one or more recipients. See Appendix A for more details on the MHS.

7.3.4 Presentation Layer

The services of the Presentation Layer are specified in the IS 8822 standard. The Presentation Layer deals with generic functions that are needed by many different kinds of applications; specifically, a common means is provided of representing a data structure in transit from one end system to another. It is important that each side of the transfer understand the content and meaning of what is being transferred. Accordingly, the Presentation Layer will take information from the applications, and convert this information into a form and structure that can be recognized and interpreted by the destination OSI end system.

Basic functions performed at this layer include: (1) data representation functions (as described above), (2) encryption functions, and (3) connection-oriented functions. Encryption deals with the way the actual data is coded or represented to provide secure data transfer. Connection functions deal with establishing, preserving, and managing the connection between two applications.

An example of the function of the Presentation Layer is indicated by the following: a Frenchman speaks French and German, and an American speaks English and German. The Presentation Layer provides the means for the two parties to recognize that they need to have their conversation in German. The Presentation Layer would convert both languages to German for communication purposes.

Presentation is described in terms of functional units, or groupings of similar functionality; these are the kernel, context management, and context restoration. The kernel refers to the connection-oriented matters mentioned above. Context management refers to defining and manipulating the format (context) of information, and context restoration refers to retrieving a context that may have been used previously. For end systems, there is sender-Presentation code and receiver-Presentation code. In sum, Presentation allows any type of system to understand information provided by any other type of system by conversion to a common information format.

The Presentation functional unit needed to support FTAM is the kernel functional unit. There is no explicit Presentation Layer for the MHS mail protocol standardized in the 1984 CCITT Recommendations; the functionality is incorporated in the Application Layer.

7.3.5 Session Layer

The Session Layer provides user-oriented services to aid in the orderly and reliable flow of information between two users in two different end systems. These services provide for increased efficiency in managing the dialogue between applications. Some functions provided by the Session Layer are error recovery (restoring information lost during underlying communication failure), synchronization (setting and resetting positions of data at each end of the connection so that each side knows where to start), and checkpointing (marking the data for convenient reference). The Session Layer protects applications and users from irregularities and problems in the underlying network.

The Session Layer protocol is also organized in terms of functional units; examples of these functional units are kernel (basic connection and data transfer) and duplex. Also included are half-duplex, expedited data, minor synchronize, major synchronize, typed data, activity management, resynchronize, and exceptions. For a further explanation of these, consult an appropriate reference in Appendix B.

There are two types of dialogue control. Either end can send data at any time (duplex) or each end can take turns sending data (half duplex). In the latter case, tokens are used to control the direction of data transfer and which process is authorized to send data. Data may be synchronized, which allows retransmission to start at a convenient point; data may also be expedited, which means that it has a higher transmission priority. Data may be typed, which allows it to be sent even if the sender does not possess the token.

FTAM and MHS have different Session requirements and options. For FTAM Session functional units required are kernel and duplex, and optional functional units are resynchronize and minor synchronize. For the MHS application Session requirements are kernel, half-duplex, exceptions, activity management, and minor synchronize functional units.

7.3.6 Transport Protocol

A pre-fabricated house is moved piece by piece from one state to a new state and reassembled properly with no damage having been done in transit. This is what the Transport protocol does with data between two end systems. The Transport Layer provides reliable, orderly end-to-end data transfer. This means that data packets are received uncorrupted and in the correct order by the Transport Layer user. The basic function of the Transport Layer is to provide the difference between the quality of service desired by the Transport Layer user and that which is provided by the Network Layer (see sec. 7.3.8).

There are many parameters that are negotiated between Transport protocols. These provide for proper flow control, proper sequencing, and proper error detection and retransmission of lost data. The international standard contains provisions for five classes of Transport service (Class 0 through Class 4). Class 4 assumes the least about Network Layer services, and is required for GOSIP systems. Class 0 is used in certain circumstances (see sec. 4.2.4 of the GOSIP FIPS).

7.3.7 Connectionless Network Protocol (CLNP)

The OSI Network Layer provides for the routing and relaying of information between nodes on the same network or interconnected networks. The Connectionless Network Protocol (CLNP) allows the network technologies referenced in GOSIP to interoperate. These include local area networks 8802/3 (CSMA/CD), 8802/4 (token bus), and 8802/5 (token ring) as well as X.25 networks. The CLNP masks the differences between these network technologies and allows these differences to be transparent to the OSI Network Layer user.

The services of the existing network technologies must be augmented to provide the OSI Network Layer service; this enhancement is also provided in the CLNP. Since the protocol to provide this service is connectionless, each protocol data unit is routed separately and the header of each protocol data unit contains addressing information as well as information relating to optional services provided by the protocol (e.g., priority and security). Work is in progress to allow the CLNP and the Connection-Oriented Network Service (CONS) to interoperate or interwork; some of the suggested methods are discussed in section 9.

7.3.8 Network Technologies

Different network technologies provide for transfer of data packets between adjacent nodes of a network. This corresponds to the Network Layer (Layer 3), Data Link Layer (Layer 2), and Physical Layer (Layer 1) from figure 8. The nodes of a wide area network are separated by long distances, whereas local area networks are usually contained within a small geographic area. This difference is responsible for the different technology used in the two types of networks. In addition, local area networks have the following characteristics: (1) ownership by a single organization, and (2) high data rate (greater than 1 megabit/second). In many cases the operation of wide area networks must depend on existing transmission facilities, such as the telephone system. The protocols that support wide area transmission in GOSIP are the CCITT X.25 protocols; local area networks in GOSIP are 8802/3, 8802/4, and 8802/5.

Issues for the Network Layer are congestion control, routing, number of steps (hops) from source to destination, and the converting of messages into packets (and vice versa). There are a number of options available for the Network Layer protocol, depending upon the precise configurations involved.

Current systems in Federal environments are vendor-proprietary and cannot interoperate. Many current subnetworks are based upon the Ethernet technology. The functionality required to transfer data packets between "adjacent" nodes of a network is provided by the Physical Layer (Layer 1) and the Data Link Layer (Layer 2).

The Physical Layer allows for the correct pin settings and signaling techniques of interfaces to lines so that bits of data may be transmitted from one machine to another machine. Issues here involve the nature of the physical medium, and insuring that proper synchronization is applied for the transfer. There are a large number of Physical Layer specifications, depending on the physical medium employed.

The Data Link Layer takes the raw transmission facility provided by the Physical Layer and transforms it into a link that appears substantially free of transmission errors to the network layer. It performs this function by taking bits and forming them into data frames; these data frames are then transmitted sequentially. The Data Link Layer provides error detection and, optionally, correction (involving two computers directly connected) across a line between nodes of a subnetwork.

The Data Link Layer checks the number and position of bits received, and performs various calculations to determine if there is an error, e.g., if a "1" bit is accidentally received as a "0". Synchronization of sender and receiver is important in this layer. The Data Link Layer emphasizes "box-to-box" communications; that is, management of bits between directly-connected computers.

7.3.8.1 CSMA/CD (8802/3)

A CSMA/CD network consists of a series of devices connected to a cable (bus). Any device on the cable may transmit to any other device on that cable, by placing the destination address on the cable, along with data. Essential steps in the CSMA/CD protocol are given below:

(1) Listen before transmitting, to ensure cable is idle.

(2) A device puts a message on the cable, indicating it wishes to send information.

(3) If that message traverses the cable intact (i.e., without encountering a collision), then that device has control of the cable and finishes sending its message. When it is finished, the cable is free again.

(4) If a collision is detected, then all transmission stops. The device must wait, and then try again at a future time using a special "back off" algorithm.

This scheme works well for low to moderate loads, because a station may transmit immediately with little chance of collision. For heavy loads, a device waiting to transmit may be indefinitely delayed, because of the frequent number of collisions encountered. This scheme is similar (but not identical) to Ethernet products that are currently in Federal offices. What the 8802/3-based products offer is minimal delay and reasonable throughput, particularly at low to moderate traffic loads. Also, CSMA/CD is fairly simple and inexpensive to implement.

7.3.8.2 Token Bus (8802/4)

The token bus technology uses a bus or cable architecture, similar to the previous local-area network, but in this instance a station needs a token in order to be able to transmit data on the line. This token is passed from station to station in a logical sequence (independent of the physical ordering). Once the station has the token, it can send data via the bus to another station for a certain amount of time; in other words, it "seizes" control of the bus for a predefined time interval. When that time expires, the station must relinquish

the token. 8802/4 buses are generally implemented using a broadband cable, although a baseband option is available.

7.3.8.3 Token Ring (8802/5)

A token ring network consists architecturally of a number of stations connected to one another via a circular cable or loop. A token travels around the ring; this token confers on a station the ability to send data. When a station wants to send, it looks for the free token; if it is available, it grabs the token, changes it to a "busy" token, and appends data to it. The data travels around the ring to the destination station(s). When the data has been received by the sending system, it is removed from the ring. After a station has finished transmitting the last bit of data, it must regenerate the free token.

The token ring scheme places no predefined upper limit on the size of a message. This method is beneficial for heavily loaded systems, because it may guarantee that a packet will send its information within a specified time (depending on the protocols involved). For lightly loaded systems, a station merely has to wait for the token to come around to begin sending, so there is minimal delay. There is no contention involved in token ring access, unlike the situation for CSMA/CD access. The primary token ring disadvantages are the complexity of the token ring scheme and the need for proper regeneration of lost or damaged tokens for the ring.

7.3.8.4 Local Area Network Bridges

Local area network (LAN) bridges are devices which connect "adjacent" local area networks of the same type (as described above) or of different types (as described above). These bridges become a component of the integrated local area network, and direct messages on the network based upon the physical (or media access control (see Appendix A)) address(es) of the devices on the local area network. This is done by consulting an address table and interpreting the machine address(es) in the data messages passing through the bridge.

LAN bridges may conceptually be defined between two or more GOSIP local area networks of the types described above. Currently, bridges between 8802/3 local area networks are prevalent. The GOSIP FIPS does not explicitly reference LAN bridges, and so their use is not precluded as long as their use does not compromise GOSIP local area network functionality.

7.3.8.5 X.25 Wide Area Network Technology

For transmission over long distances, existing public network facilities are usually used. Since there are so many types of devices that could be attached to such systems, it is desirable to standardize protocols for network access by these systems. The X.25 protocols fill this need. X.25 defines an interface between a DTE (data terminal equipment) and DCE (data circuit-terminating equipment). The DCE is the network interface point (owned by the network), and the DTE corresponds to user terminals (owned by the user).

The X.25 protocol establishes a virtual circuit between two machines; this is a definite path connecting the two machines through intermediate machines. This path is valid for the lifetime of the connection. Source and destination addresses, as well as other information, are put on a call setup packet; data packets follow.

The X.25 packet layer (layer 3) protocol is concerned with data format and meaning in a frame, as well as routing and virtual circuit management. When one system wants to connect to another system, a logical circuit is set up between them; there are a number of parameters which specify various kinds of information. Some functions are: reset, and clearing a circuit (when a call request cannot be completed). The restart command clears all virtual circuits between specified DTE and DCE.

Currently in the Federal environment, versions of X.25 dated 1980 or before are in place. The 1984-based X.25 protocols offer enhanced capabilities to support OSI applications, such as Network Layer addressing

and quality of service provision. GOSIP requires 1984 X.25 in Version 1; it is expected that in a later version 1984 X.25 or 1988 X.25 will be supported. In the very short term, pre-1984 X.25 may be allowed for practical reasons; however, vendors must commit to provide 1984 X.25 functionality as soon as possible for GOSIP compliance.

7.4 Implementation Alternatives

7.4.1 General

The way an interface will be implemented depends to a certain extent on the way the adjacent protocol layers are implemented, and to a great extent on the operating system environment. Basically, there are two categories: an open interface, and an embedded interface. An embedded interface is "invisible" to program users. The protocols are enmeshed and entangled so that there is no clear boundary between them. In an open interface, there appears to be a clear, well-defined boundary separating two distinct pieces of code. Figure 10 illustrates this.

It is important to understand that the OSI architecture gives vendors great flexibility in determining how the protocol standards are implemented. The interface that is specified between adjacent layers is an abstract definition that was created in order to describe the services that the lower layer offers to the upper layer. However, vendors are not bound to implement discrete processes corresponding to the functionality of each layer with accessible service interfaces between the layers. For example, a vendor may decide for reasons of efficiency to merge the functions of the Presentation and Session Layers in one process without an exposed interface between the layers. As long as the protocol information that is transmitted between the Presentation and Session Layers of the local system and the communicating end systems can be interpreted by both systems, the implementation conforms to the international standards for these protocols.

Users may have reasons to request that the vendor provide an accessible interface to one or more layers in their implementations. An accessible Transport Layer interface allows a user to write software which uses the services of OSI layers 1-4 to reliably transfer data between different end systems. This software may use nonstandard protocols which can be interpreted by the communicating end systems. An accessible interface to the Association Control Service Element (ACSE) allows different applications to access the ACSE to perform common application layer services, as described in section 7.3.1. An accessible interface to the MHS Message Transfer Agent allows users to write their own User Agents which use the services of the Message Transfer System to transfer information to each other.

The OSI end system functionality need not and frequently will not be implemented on one stand-alone processor. For example, implementing OSI layers 1-4 on a front-end processor can free a central processor from the input/output overhead and allow it to perform other tasks more efficiently. The front end processor is also able to act as a concentrator servicing more than one mainframe. The user interface and the application layer functions for FTAM and MHS can be implemented on terminals or workstations which access a central processor for lower-layer services. The benefits and tradeoffs for each implementation alternative will vary with the situation and they should be examined carefully while configuring an OSI system.

7.4.2 MHS Implementation Choices

The User Agent can be implemented in the same processor as the local Message Transfer Agent or in another processor at a remote location. The User Agent can be supplied by the same vendor that supplied the Message Transfer System or by a different vendor. The User Agent and Message Transfer Agent can be consolidated in one processor with access to the User Agent by desk-top personal computers provided by non-standard terminal emulator software. There are many options for configuring a Message Handling System and the advantages and disadvantages of these options will vary with each Federal agency. Procurement authorities should be aware of the options and, if nesessary, consult with vendors about available alternatives before issuing a solicitation document.

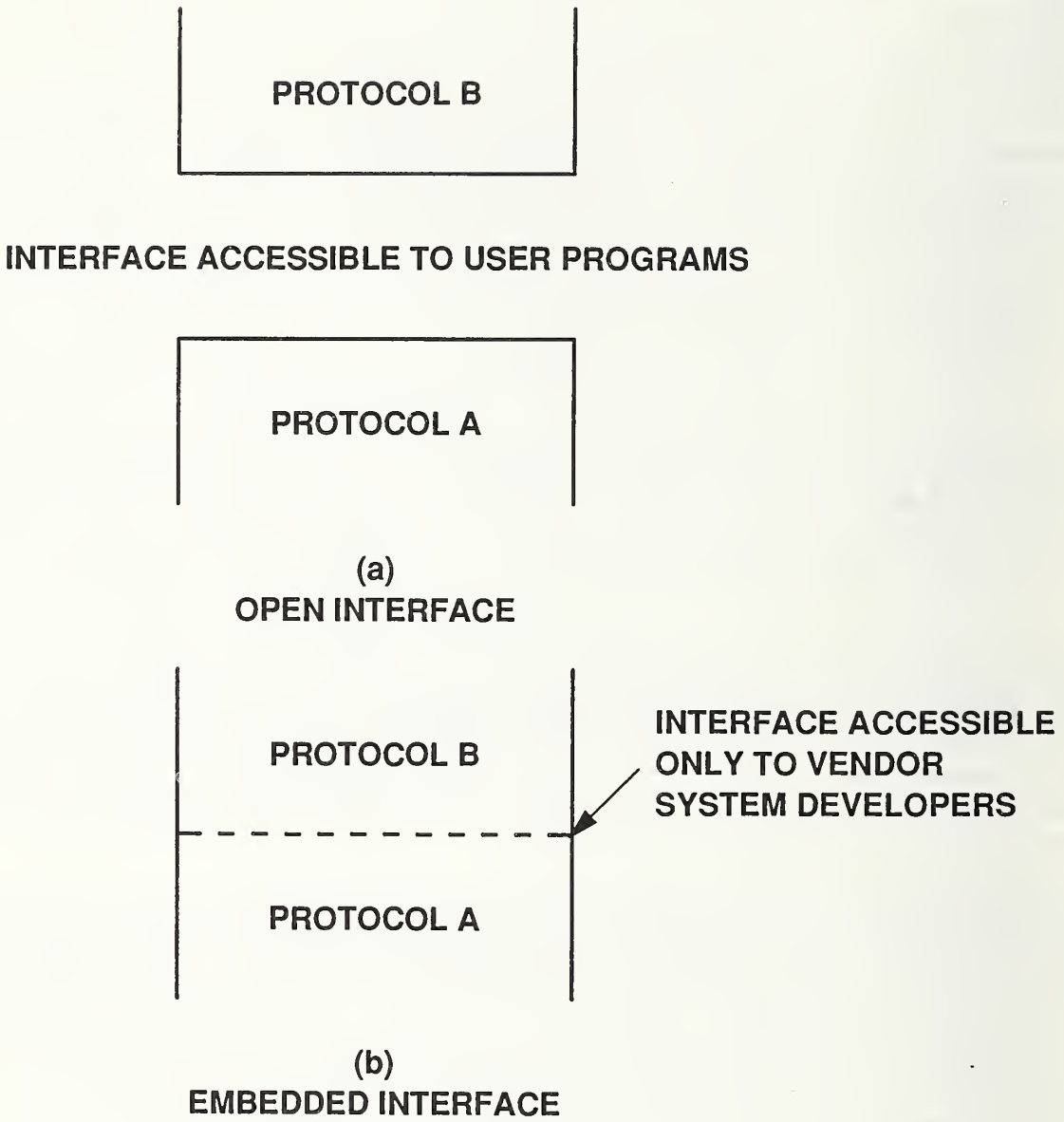


FIGURE 10
OSI SERVICE INTERFACE CHOICES

All User Agents provide services which are not subject to standardization. User Agents assist the originator to create and edit a message and store the message until the recipient is ready to read it. Federal agencies that have specific requirements for nonstandard User Agent services should specify these requirements in solicitation documents.

The Message Transfer System and the Interpersonal User Agents (see Appendix A) provide the capability of transferring electronic mail between human users. Other special-purpose User Agents can be written which use the services of the Message Transfer System, if the vendor provides a means for these User Agents to interact with the Message Transfer System. Federal agencies that have a requirement to write or procure their own User Agents should specify that a programmable interface to the Message Transfer System is required in their solicitation documents.

Vendors who have previously marketed electronic mail systems may preserve their existing user interface when building MHS products. The system will be programmed to recognize when a recipient address is nonlocal. Special relay routines will then format the message in accordance with the CCITT MHS Recommendations. Preserving the existing user interface has the advantage of requiring a minimum of training for users of the old system; however, in this case, the ability for a user to generate certain optional Interpersonal Message service elements (e.g., Expiry Date, Cross-Reference Indication) may not be provided. Procurement authorities should be aware of these optional Interpersonal Message service elements (see Appendix A) and insure that services that are critical to their mission are specified in solicitation documents.

The MHS Recommendations describe body parts other than IA5 (ASCII) text. Accordingly, users should have the capability of specifying that their Interpersonal User Agents will be able to process body parts other than IA5 text.

The NIST Workshop Agreements [NIST 1] allow limited flexibility in the Transport and Network Layer services used by MHS implementations. Procurement authorities should specify that Transport and Network Layer services they require when procuring a Message Handling system. For an expanded discussion see Appendix A.

Implementations of Session (and Transport) supporting MHS could be bundled or separate from each other and from MHS implementations. Session or Transport could be implemented on a front-end processor, communications processor, or on each host. Sender and receiver portions could be implemented together or separately. Figure 11 gives some implementation styles relating to the MHS protocol.

7.4.3 FTAM Implementation Choices

FTAM may be viewed as a series of callable library routines designed to serve other applications or processes. There is no standard FTAM user interface; the applications manager may request a special user interface to accommodate individual requirements. FTAM may also be integrated into existing file transfer software and/or remote file systems.

FTAM may be implemented in terms of the initiator or responder (or both), and in terms of a sender or receiver (or both). FTAM may be implemented on a front-end processor, communications processor, or on a host or workstation. FTAM functionality may be available directly or remotely; for example, FTAM does not have to be implemented on every PC, since these services may be made available in other ways. FTAM may be integrated directly in a local system environment (operating system), or separately.

It might be more cost effective to implement an FTAM product on a central processor, rather than on each individual host, particularly if the number of hosts is large. A host-to-front end protocol could then handle the conversion between an existing file protocol on each host and FTAM. This means that code on each host would not have to be changed to accommodate the installation of the FTAM protocol on each host.

As a convenience to users, FTAM defines special functional profiles called Implementation Profiles.

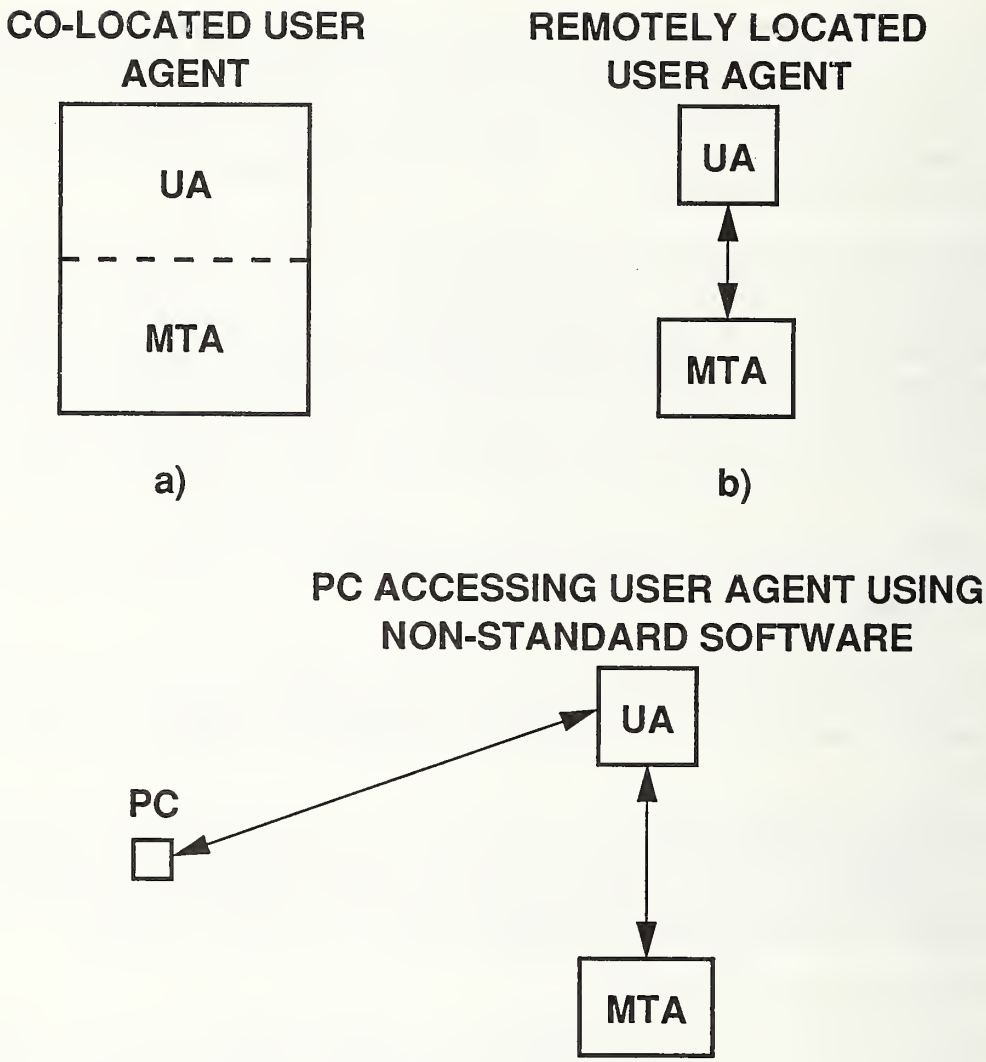


FIGURE 11
MHS IMPLEMENTATION CHOICES

There are six Implementation Profiles defined: Simple File Transfer (T1), Positional File Transfer (T2), Full File Transfer (T3), Simple File Access (A1), Full File Access (A2), and Management (M1). One category in each class may be selected (e.g., T2, A1, and M1), or a category may be excluded (e.g., A1).

These Implementation Profiles are defined in terms of service classes, attributes, and document types. A user would evaluate conformance claims to one of these profiles based upon requirements stated in the NIST Workshop Agreements [NIST 1]. The simplest profile is T1; support of this is required of all FTAM systems. In general, higher-numbered profiles are supersets of lower-numbered profiles in the same class. For a maximum set of FTAM functionality, a user would require T3, A2, and M1.

Descriptions of what the profiles contain are given in the NIST Workshop Agreements. Each profile contains a set of functions which can be directly evaluated. For example, an inventory control system would include T2, A1, and M1, whereas a spooling application would require only T1 and M1. Each of the Implementation Profiles contains optional features as well.

FTAM may be "bundled" with any other modules, or exist as a separate module. In certain cases, FTAM cay be completely integrated with an existing file system, either local or remote. Implementations may use either an "external" or "internal" file service.

For a multi-user computer system, one might implement the kernel, storage, and security virtual filestore subsets. For a centralized database system, one would also implement the kernel, storage, and security subsets.

Some local issues for the user to consider are: extensibility, timer values, data item size, and efficiency, as well as synchronization. Other issues to consider are filesize, file naming, concurrency control, security, access control, audit capability, encryption, and error recovery.

The FTAM initiator and FTAM responder may be implemented together or separately depending upon particular agency configurations. Implementation profiles have been defined to enable users to implement FTAM more efficiently. Server implementations are defined in terms of file servers and print servers, among others. File servers may be implemented on a variety of different devices, and would just involve responder functionality in most instances. Print servers offer a more limited set of capabilities, and could be implemented on various special-purpose devices. For more FTAM information, consult Appendix A.

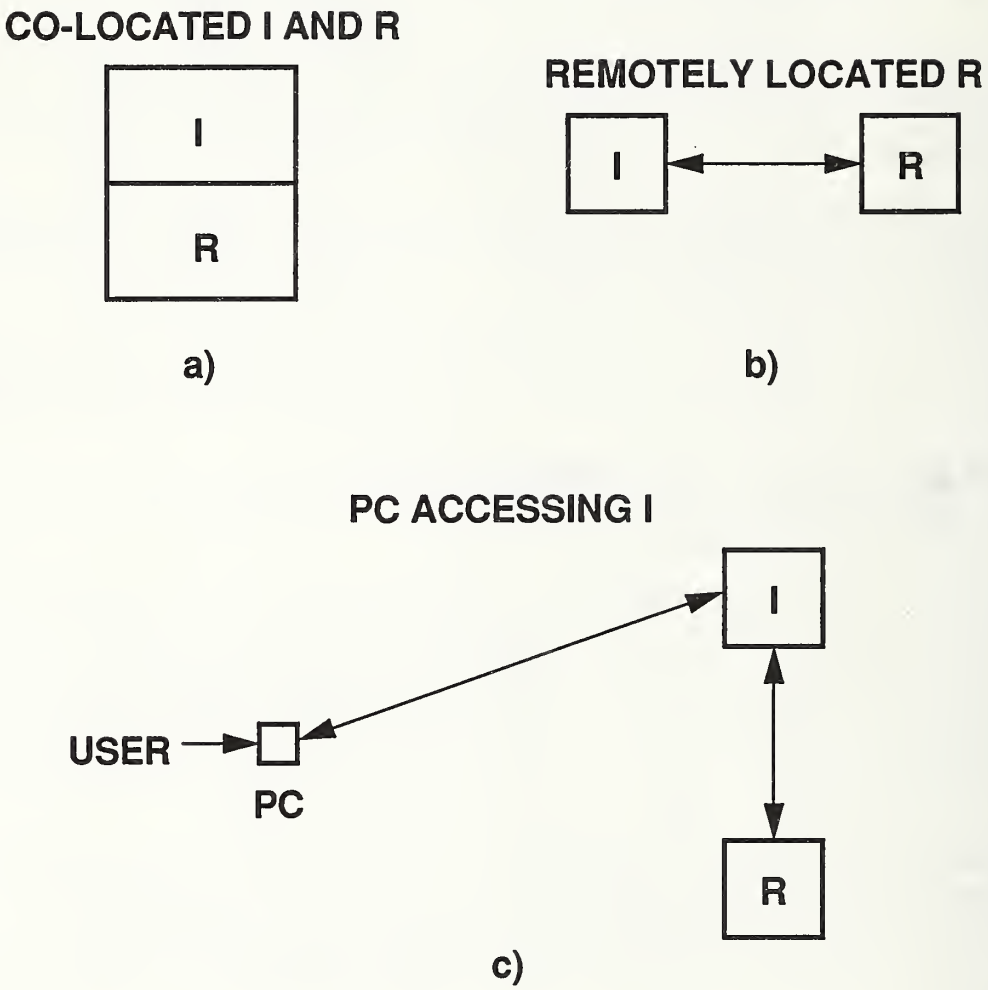
Presentation and ACSE code may be implemented together with FTAM (or with each other) or separately. Presentation or ACSE may be implemented on a host, front end processor, or communications processor. Functionality may be available directly or remotely. Sender and receiver code may be implemented together or separately. Transport and/or Session code supporting FTAM may be implemented together with FTAM or separately as well. Figure 12 gives some implementation choices relating to FTAM.

7.4.4 Performance

Each agency must determine specific performance requirements, if any, for inclusion into RFPs citing GOSIP. For each protocol considered (e.g., X.400, FTAM, end-to-end transport) different performance criteria may be of interest. Performance measures of general interest usually include delay, throughput, capacity, response time, availability, and reliability. Of course, to be measurable such performance parameters must be precisely defined.

The NIST is working to develop performance and functional evaluation guidelines for GOSIP. The guidelines are scheduled for completion in 1990. Previous work completed by the NIST is available now, but focuses only on end-to-end transport performance. Until the NIST guidelines are complete, agencies may desire to work directly with the NIST on specific procurements.

Two possible levels of performance to consider are: end-to-end (Transport Layer) performance, and application-level performance. Some factors which may affect performance at the Transport level are: net-



I = FTAM INITIATOR
R = FTAM RESPONDER
PC = PERSONAL COMPUTER

FIGURE 12
FTAM IMPLEMENTATION CHOICES

work diameter, window size, network load, packet size, and error rate.

Currently performance is not standardized under the scope of the OSI Reference Model. Agencies should develop performance criteria based upon internal needs. Important performance metrics and benchmarks for a particular agency should be defined. Then, with vendor consultation, it should be determined what is practical and achievable, given current architectural and technology constraints.

Application-level performance requirements should include measurements of user-to-user throughput and acceptable end-user delay time under a set of typical loads. An end-system user may also be interested in a measure of reliability or robustness for a particular application. A typical performance metric to consider is static capacity of a system (e.g., the number of simultaneous connections). When performance data is available, this information may assist in precisely defining performance requirements in solicitations.

7.5 Technical Information in Product Announcements

Technical information in vendor product announcements will stress the OSI-based services provided. Both OSI terminology and vendor-specific terminology are likely to be employed. Upon receiving a product announcement (or a response to a solicitation), the technical specialist should examine and interpret it in the following manner: (1) make a list of essential agency OSI functional requirements, (2) make a list of OSI services provided by the vendor, (3) match the two above-defined lists to determine whether all of the agency's functional requirements are satisfied, and (4) consult this Guide (and other appropriate documents) to understand the technical material in the announcement. It is possible, upon performing this list comparison, that product features will emerge that were not on the "agency requirements" list; if this is true, then these could be added to agency requirements.

Agency officials should ensure that vendor enhancements to the GOSIP FIPS (1) do not compromise basic OSI functionality, and (2) do not adversely affect GOSIP interoperability. Subject to these constraints, users may request and encourage enhancements to GOSIP-compliant products from vendors.

7.6 GOSIP Application Information Flow

This section will reference the two Application Layer protocols (FTAM, MHS) contained in the GOSIP FIPS.

7.6.1 FTAM Example

The steps to accomplish an FTAM activity are listed below.

(1) A user issues an FTAM initialize service primitive, with the appropriate parameters included.

(2) After success, an FTAM select is issued if a pre-existing file is to be selected; otherwise an FTAM create is issued if a new file is to be created.

(3) After success, an FTAM read attribute is issued to interrogate the properties of the file; an FTAM change attribute may be issued to change the properties of the file.

(4) An FTAM open may be issued to gain access to the contents of the file. The context and format of the file is negotiated at this time.

(5) An FTAM read or FTAM write is issued, depending on whether the file is to be read or written. FTAM data commands transfer data. FTAM "data ends" terminate the data flow in one direction, and FTAM "transfer ends" terminate the total data transfer. FTAM cancel interrupts an existing data transfer.

(6) An FTAM close releases access to the contents of a file.

(7) An FTAM "deselect" releases access to the file's properties; an FTAM delete eliminates the file.

(8) An FTAM terminate ends the file activity normally. An FTAM abort abruptly ends the file activity (because of an error).

7.6.2 Message Handling Systems (MHS) Example

In a Message Handling System, or X.400 implementation, the steps taken by a process wishing to send mail to a recipient process are listed below.

(1) The originator specifies the message to be sent, to whom it should be sent, and which Message Transfer services are being requested (e.g., priority delivery or delivery notification).

(2) The user agent submits the message to the local MTA. The MTA accepts responsibility for delivering the message to all recipients.

(3) The MTA acts like a post office and relays the message to other MTAs depending on the destination address. This message may cross different management domains.

(4) A message consists of an envelope and contents. The information that the Message Transfer System normally needs to perform its task is on the message envelope. The Message Handling System does not examine the contents, except in rare instances, to convert the encoding of the message.

(5) When the message gets to the destination MTA, that MTA will recognize the address and deliver it to a local user agent.

(6) The user agent will attempt to deliver the message to a recipient, or store the message for later delivery.

(7) If there is a problem with delivering the message to the user agent, a nondelivery notification will be returned.

7.7 Future GOSIP Protocols and Services

Given below are descriptions of protocols under development and for incorporation into future versions of GOSIP. The appendices of the GOSIP FIPS give additional detail and scheduling information. Users should consider this information when making long-term procurement plans.

7.7.1 Transaction Processing (TP)

Transaction processing is an Application Layer protocol which is used for exchange of information between two or more distributed systems according to the ACID rules. ACID, as applied to a transaction, ensures: (1) atomicity (the total work is performed or nothing is done), (2) consistency (work is performed accurately and correctly), (3) isolation (while the work is being performed data is not available to other transactions), and (4) durability (the work is fault-tolerant). This last point is especially important in the context of data base management. It means that enough information will be retained so that in the event of a system failure the information on the data base will be unaffected A situation where transaction processing might be applied is given below.

An individual desires to fly to a specific city on a specific airline at a set time; that individual may also want to rent a certain car, stay at a certain hotel, apply for an advance, and see some clients. Without TP the traveller would have to make a separate reservation with the airline, with the car rental company, and with the hotel, as well as with the bank and clients. Each of these is a separate action; if there are problems with any one action, a drastic change in plans may be necesary. With TP, that individual would be able to first find out whether all of the actions could be completed successfully, and if they could, then that individual could direct that they be carried out as a single action. Other potential uses for TP are in banking transactions and supply and accounting systems.

7.7.2 Secure Data Network Service (SDNS)

The Secure Data Network Service (SDNS) incorporates a set of security protocols and procedures that provide a number of security services in the OSI Reference Model (IS 7498/1) [ISO 1]. The SDNS is an example of implementing security in accordance with the OSI Security Architecture [ISO 15] that has recently been approved as an International Standard. The Security Architecture defines a number of security services that can be implemented at one or more layers of the OSI architecture.

The security services that are defined in the OSI Security Architecture and provided in the SDNS are: authentication, access control, confidentiality and integrity. Procedures for providing the nonrepudiation security service are still under development. Protocols and procedures for providing specific security services at layers 1, 3, 4, and 7 are being developed for the SDNS. Specific algorithms for confidentiality, integrity, authentication, and key distribution have been specified.

The SDNS can be used in a variety of networks including local area networks, wide area networks and point-to-point communications networks. The SDNS offers comprehensive security in a number of network applications including electronic message handling and file transfers. The SDNS is intended to serve as the basis for protecting classified data as well as unclassified , but sensitive, data in a wide range of applications.

7.7.3 Network Management

As the number of networks and related services grows throughout the U.S. Government during the 1990's, requirements for integrated network management capabilities will become more urgent. Specifically, network operators will need to configure network resources, detect and correct faults, account for network use, monitor and adjust performance, manage security mechanisms, and secure network management information. Network components projected to be employed include GOSIP end systems and intermediate systems, ISDN switches, X.75 gateways, PBXs, modems, multiplexers, packet switches, leased point-to-point circuits, and local area networks.

The NIST intends to work for an environment where network components made by a variety of vendors can be managed from an integrated network manager. This will require (1) defining a set of interoperable protocols for exchanging management information, (2) agreeing on the structure of managed objects, and (3) defining the managed objects and related attributes. The NIST plans to issue a network management FIPS. The protocols for exchanging management information will be a subset of those found in GOSIP, augmented with additional appropriate OSI protocols. The managed objects, attributes, and structure in the network management FIPS will be worked out with industry and user participation in standards meetings and other open forums.

The first NIST goal is to produce an interim network management FIPS for use in advance of a complete solution. The second network management FIPS should be based on completed international standards.

7.7.4 Integrated Services Digital Network (ISDN)

Integrated Services Digital Network (ISDN) provides the capability of combining voice, video, and data communications over digital lines at moderate to high data rates. ISDN provides end-to-end service across this digital network

The services that ISDN will provide to the Federal GOSIP user are high-bandwidth capability and a reliable lower layer network technology. In the future the upper layer OSI protocols will be able to run over ISDN technology, as a "backbone" end-to-end connectivity service. In addition, ISDN technology may be applied to uses that are not OSI-related. For more on ISDN, see section 10.

7.7.5 Fiber Distributed Data Interface (FDDI)

Fiber Distributed Data Interface (FDDI) specifications describe a token passing technology allowing for very high data rates over fiber optic links connecting systems. Instead of the 5-16 Mbit/sec data rates over typical local networks, data rates of up to 200 Mbit/sec are achievable using FDDI. Applications for this technology can include weather information processing systems, oil refinery drilling operations, and the space shuttle support program. End systems and software must be designed to effectively handle high-bandwidth FDDI transmission. FDDI systems can be useful in connecting local-area and wide-area network facilities in Federal environments.

7.7.6 Dynamic Routing

Currently, routing tables are static; that is, a route to the destination address is computed at intermediate systems using routing tables which can only be modified by static means. Dynamic routing will allow the most efficient route to a destination to be selected, based on such factors as congestion, path availability, and line charges. The protocols to perform this function are the intermediate system to intermediate system (IS-IS) protocols, and the end system to intermediate system (ES-IS) protocol.

The ES-IS protocol provides the capability for end systems and intermediate systems on a subnetwork (e.g., a single 8802/3 local area network) to locate each other. IS-IS protocols provide for the dynamic routing of information between different subnetworks that are under the control of the same or different administrative domains.

7.7.7 FTAM Extensions

In the future, the FTAM standard will be augmented to allow: (1) simultaneous reads and writes to a file (for use in database applications), (2) file directory manipulating capability (ability to search (list) directories), and (3) specification of different levels of access control on portions of files. These extensions will increase the flexibility of applications that may use FTAM.

7.7.8 X.400 (MHS) Extensions

The Message Handling Systems (MHS) specifications in Version 1 of GOSIP are based on the 1984 CCITT Recommendations. The GOSIP MHS extensions will be based on the CCITT 1988 Recommendations. Services that will be considered for future versions of GOSIP include security, message store delivery, use of directory services (see sec. 7.7.9) and an OSI architecture which includes ACSE and the Presentation Layer.

The security features include message originator authentication, checks against unauthorized disclosure and verification of content integrity. Message store delivery allows personal computers without full User Agent functionality to access MHS services.

MHS implementations conforming to the 1984 Recommendations sit directly above and use the services of the Session Layer. Implementations conforming to the OSI architecture specified in the 1988 Recommendations will be upwardly compatible with the earlier implementations.

7.7.9 Directory Services

The ISO is expected to issue the Directory Services specification as an IS (International Standard) during 1989; the CCITT has approved the release of a similar but not identical Recommendation in late 1988. The Directory Services Protocol provides a facility for storing and retrieving information about objects in the OSI environment. For each object the Directory maintains an association between the object's name and its attributes. Examples of standardized attributes for processes are OSI service access point addresses and electronic mail originator/recipient names. Typical attributes for a Directory entry on an individual include electronic mail name, telex number, telephone number, facsimile address, and postal address.

Using the Directory to provide addressing information about an object based on the object's name can shield OSI users from underlying changes in the network. A limited browsing facility is supported to aid users in identifying names. The Directory also supports a "yellow pages" service, capable of providing users with names of all objects having specified attributes (e.g., all devices connected to address 0123).

7.7.10 Virtual Terminal Protocol

The Virtual Terminal Protocol allows terminals and hosts on different networks to communicate without requiring that one side know the terminal characteristics handled by the other side. A generic set of terminal characteristics is defined which is mapped to local terminal characteristics. A set of parameters developed to describe a particular type of terminal is called a profile. Standardized profiles under development include TELNET, transparent, forms, page, and scroll.

7.7.11 Connection-Oriented Network Service (CONS)

The Connectionless Network Protocol (CLNP), mandated in GOSIP, allows different types of networks to interoperate; however, the CLNP introduces certain inefficiencies when two communicating end systems are located directly on the same logical X.25 subnetwork. Use of the CONS can improve efficiency when operating over a single logical subnetwork (e.g., a single X.25 network or a set of X.25 networks interconnected by X.75 devices). The CONS is not precluded as an option in Version 1 of GOSIP. Version 2 of GOSIP will specify procedures for using CONS to achieve interoperability. The optional use of CONS does not remove the requirement for GOSIP-compliant systems to implement the CLNP as the basic Network Layer protocol.

8.0 REGISTRATION PROCEDURES

8.1 Motivation for Registration

In order to communicate, it is necessary to identify the objects involved in communication. These objects have names and addresses. A name is a collection of attributes that identify an object within an authority domain. An address is a name that is used to specify the location of an object. Both name and address attributes are assigned hierarchically.

Without registration authorities, chaos will result, with random name and address values being assigned to objects. Since systems would not be able to uniquely identify themselves globally, communication would become impossible. Verifying the existence of connections would become impossible; routing of protocol information would become cumbersome. For all of these reasons, registration procedures are essential in the OSI environment.

If an organization does not communicate with "outside" organizations (where "outside" is agency-specific), then an organization does not have to be bound by any addressing recommendations contained herein. However, if an organization intends to communicate with "outside" organizations, then the recommendations in this section comprise a viable consistent mechanism for assigning values.

The philosophy of all OSI registration is the same; for an understanding consult section 8.2. Several objects need to be registered for the GOSIP FIPS. These are described in sections 8.3 and 8.4. For planning purposes, objects which will need to be registered in future GOSIP versions are mentioned in section 8.5. Section 8.6 gives a list of general registration guidelines. Finally a summary of required actions for users is given in section 8.7.

8.2 Theory of OSI Address Assignment

OSI names and addresses consist of attributes which are hierarchical in nature and which combine to uniquely identify or locate an OSI object. Since the relationship between the components of a name or address is hierarchical, it follows that the registration authority for names and addresses should also be hierarchical. A governing organization does not always have sufficient knowledge of organizations lower in the hierarchy to wisely assign values within those organizations. Thus, an approach frequently taken is to delegate registration authority to the lower organizations.

Hierarchy implies a "treelike" structure where the number of objects increases from the "top" of the tree to the "base" of the tree. The tree may be sliced into horizontal "levels"; level one corresponds to the "top" of the tree, and the highest-numbered level corresponds to the "bottom" of the tree (or base). At the top of the tree, there is one designator that is most "powerful"; that is, it has the greatest scope of authority (largest domain). This designator assigns identifier values to objects under its authority. These objects have smaller domains than the objects immediately above. Each of these objects has a smaller scope of authority than the objects immediately above. This process goes on continuously, moving down the tree. Figure 13 illustrates this concept.

Important concepts are that the scope of authority decreases as one moves down the tree, and that the number of objects increases as one moves down the tree. One authority at a specific level may create zero, one, or many subauthorities at the next higher level. The number of levels in such a treelike structure is arbitrary.

Taking a path through the tree from "top" to "bottom," and collecting all the identities moving from top to bottom, one constructs a sequence of attributes which may be read from left to right to get a unique specification for an object. For example, the indicated path in figure 14 may be read as the sequence of attributes "ISO, ANSI, NIST, SYS X."

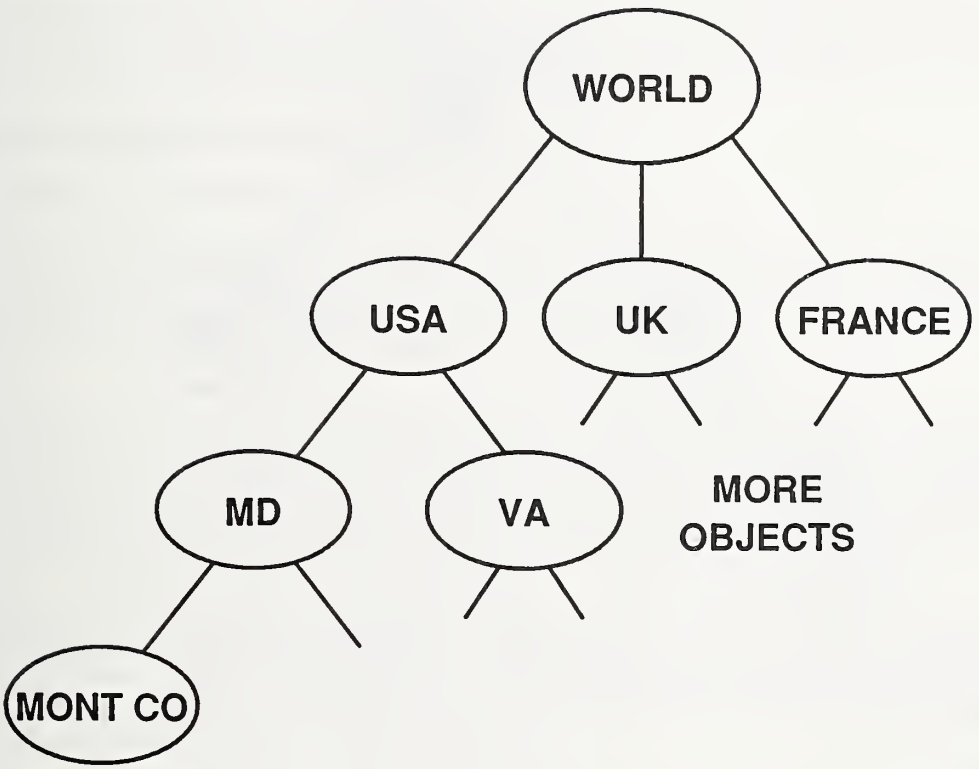


FIGURE 13
HIERARCHICAL TREE STRUCTURE

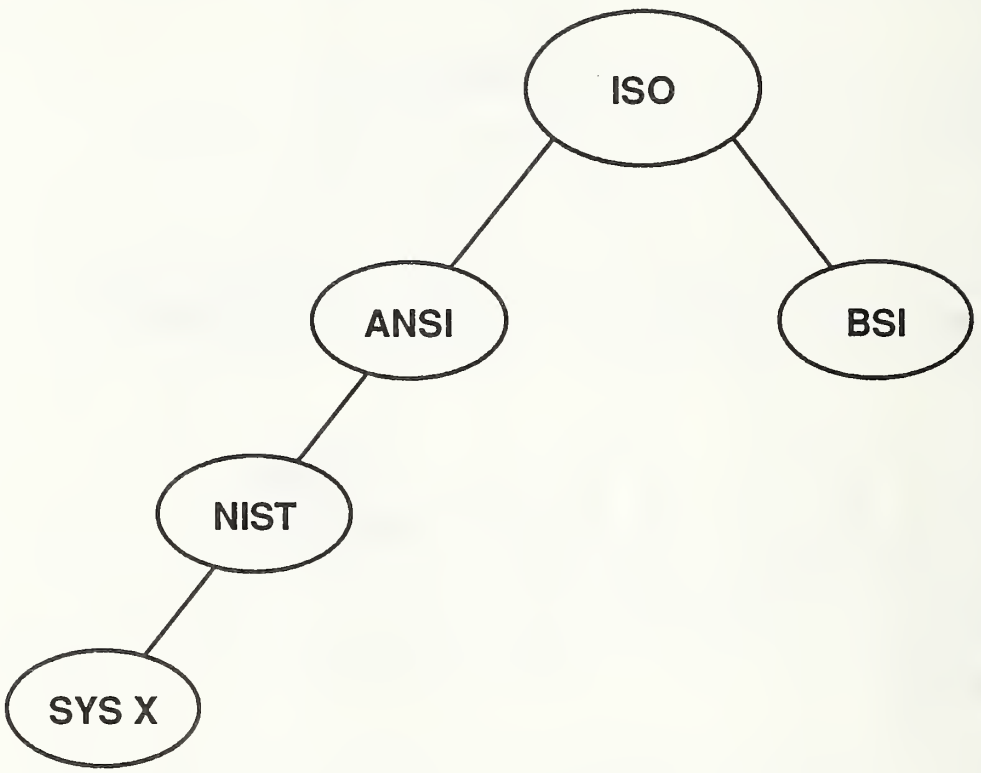


FIGURE 14
SAMPLE REGISTRATION STRUCTURE

No one element in the sequence is necessarily unique, but all the elements considered together in the proper order are unique as a group. Also, each element with the same immediate parent is unique at its level. The term "sequence" implies a definite ordering of elements. To create a unique sequence, an ADP system may "pick off" elements in a path down the tree, and append each selected element to the end of the list of previously-selected elements. To decode or "parse" a unique sequence, an ADP system will read the elements of the sequence in the order encountered from the beginning of the sequence, and construct a "path" in the hierarchical identification tree.

This above-defined hierarchical process will be applied to evaluate and resolve identification for each of the important object classes under consideration in sections 8.3 through 8.5. The advantage of such an approach is that it provides a convenient mechanism for expressing uniqueness without overburdening any one particular level of authority.

An important consideration applicable to real systems is that the minimum amount of information should be retained at any one point to accurately identify any other point. This strategy avoids unnecessary storage costs and complex encoding and decoding algorithms.

8.3 Network Service Access Point (NSAP)

8.3.1 Background and Importance

In the OSI Reference Model, reliable data communications occur between two end systems, usually via one or more intermediate systems. End systems are terminus systems, where data originates or is finally received. Intermediate systems are "transit systems," through which information passes from one end system (source) to the other end system (destination).

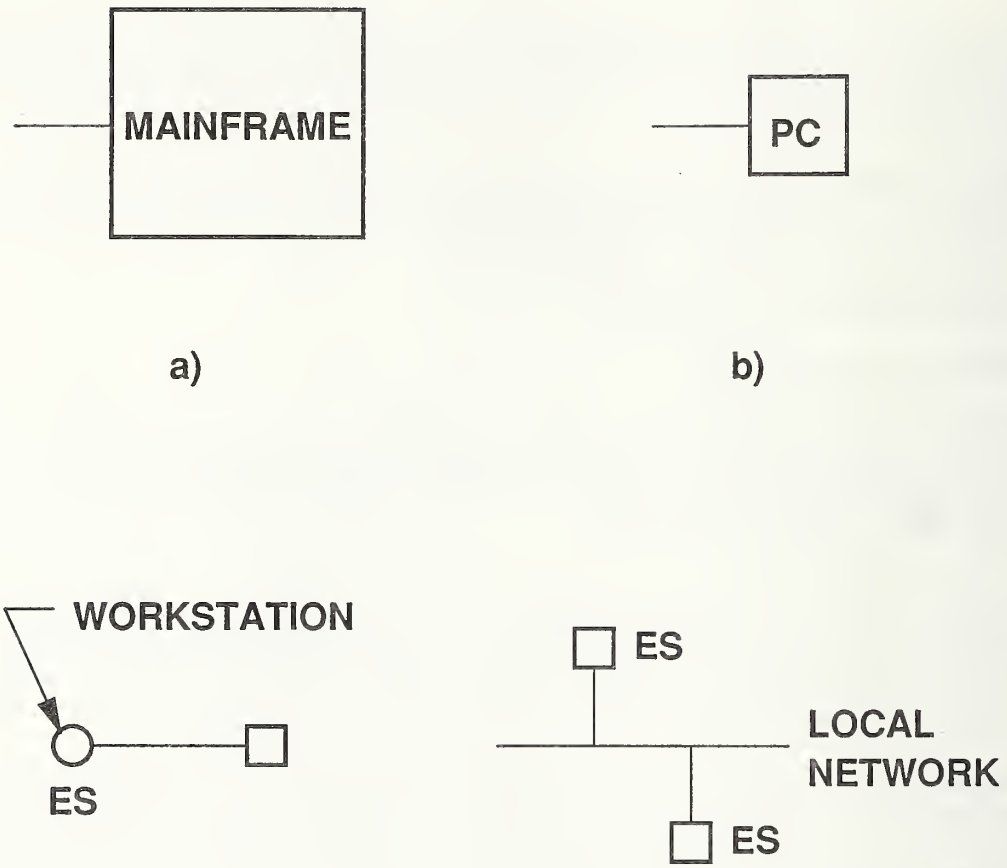
The terms "end system" and "intermediate system" refer to roles in transmittal of data and not to any special configurations. A system may be an end system or an intermediate system at different times; such systems may be attached to local area networks or attached to wide area networks. Intermediate systems are used to interconnect subnetworks in OSI communications. An end system is usually controlled by a single authority. Any of the configurations shown in figure 15 may qualify as an end system.

Intermediate systems are used to link together subnetworks to provide a path connecting end systems. An end system may be connected to more than one subnetwork; similarly, a subnetwork may have multiple end systems connected to it. Figure 16(a) illustrates this in a typical Federal environment; figure 16(b) shows the linking of subnetworks in a chain to connect two end systems. The actual physical connections are labeled as subnetwork points of attachment (SNPAs).

The NSAP identifies end systems to one another in a network of systems; the identification is necessary because a packet of information sent from any source system must include a destination system identifier. An intermediate system will "read" the NSAP address and determine where to send the packet (a similar function to that of a post office in reading an address for an envelope). Each NSAP is unique globally in the context of OSI; an NSAP value is disseminated to all other systems communicating with this system. The NSAPs themselves only have meaning to the "end" systems (source and destination) in terms of providing the OSI Network Layer service.

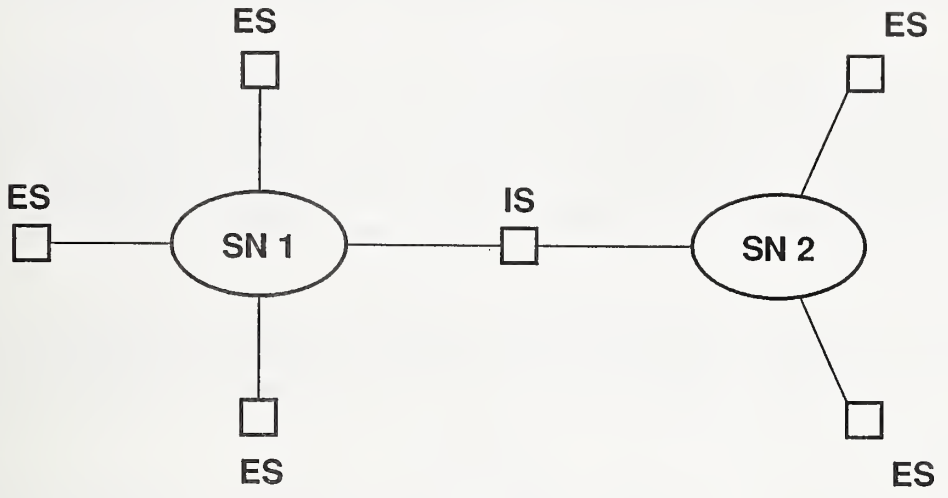
The NSAP also identifies a point at which service is provided to the Transport Layer, which is responsible for the reliable end-to-end transfer of data in the OSI model. There may be any number of NSAPs for an end system. These NSAP values must be known to the "end-to-end" communications software. NSAPs are encoded as unique strings of characters (or numbers) that may be interpreted reading from left to right using the hierarchical model described previously. Each NSAP value in an end system specifies a different user of the Network Layer service.

From figure 16, intermediate systems route information based upon selected components of NSAPs received in transit. If the NSAP "matches" the system address, that system is in fact the destination

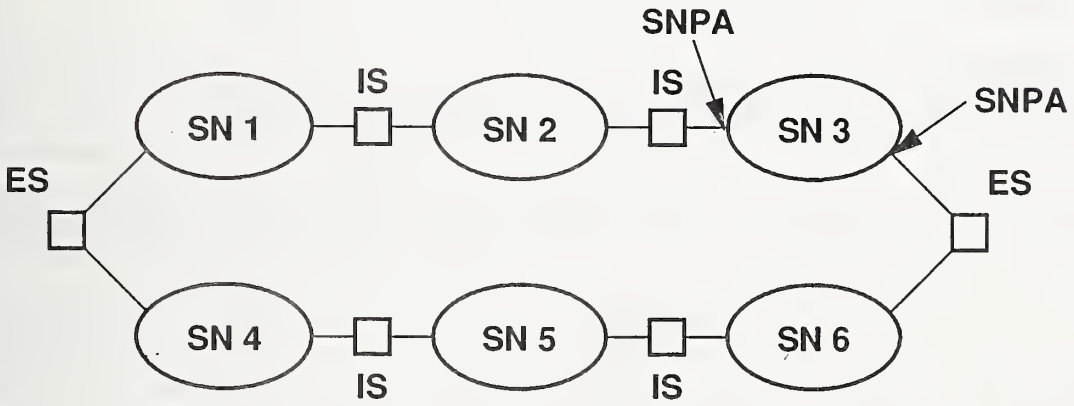


ES = END SYSTEM
PC = PERSONAL COMPUTER

FIGURE 15
END SYSTEM EXAMPLES



(a)



(b)

SN = SUBNETWORK
ES = END SYSTEM
IS = INTERMEDIATE SYSTEM
SNPA = SUBNETWORK POINT OF ATTACHMENT

FIGURE 16
INTERMEDIATE SYSTEMS AND SUBNETWORKS

system. If not, then a routing table is used to find the next system in the routing process.

In a typical Federal environment, there is usually a mix of different proprietary systems (public and private, local and long-haul) connected at a variety of different points using a variety of different addressing schemes. It will be necessary for Federal agencies to (1) determine end systems (users of the network service), (2) identify critical SNPAs, and (3) reconcile pre-existing subnetwork addressing schemes in arriving at an NSAP value.

The NSAP is the only address in OSI that identifies end systems uniquely; all other OSI addresses identify intermediate systems or end-system processes. It is important to be able to specify NSAP addresses globally in the Federal environment because an increased communication capability is possible across different subnetworks in a distributed environment. If every end system in all Federal agencies is assigned a unique address, then every end system, from PC to mainframe, can potentially communicate with every other end system.

In sum, an OSI network is composed of end systems on different subnetworks interconnected by intermediate systems. NSAPs identify the end points of communication, or the users of the Network Layer. The NSAP selector (see sec. 8.3.3) allows different users of the Network Layer service to be differentiated.

8.3.2 NSAP Format

The NSAP (Network Service Access Point) addressing structure allows for a maximum length of 20 octets or 40 decimal digits. The format of NSAP addresses for GOSIP is given below.

Since GOSIP specifies a connectionless network service, source, and destination NSAP addresses appear in the protocol control information (PCI) of appropriate protocol data units (PDUs) used when providing the network service. The U.S. Government NSAP address structure is shown in figure 17.

The U.S. Government NSAP address is hierarchical. The principal components are the Initial Domain Part (IDP) and the Domain Specific Part (DSP). The IDP is divided into the Authority and Format Identifier (AFI) and the Initial Domain Identifier (IDI).

The AFI value of decimal 47 means that the DSP part of the address is represented in binary rather than decimal digits. It also means that the IDI part is interpreted as a four decimal digit International Code Designator (ICD). The ICDs are allocated and assigned by the ISO. An ICD identifies an organization that is the Address Registration Authority for a subdomain; thus, it is responsible for structuring and for allocating and assigning the values of the DSP.

The National Institute of Standards and Technology (NIST) is the Address Registration Authority identified by IDI values 5 and 6 under AFI 47. Code 5 will be available for use by the entire Federal Government. The NIST will allocate and assign DSP values for the IDI code 5. The NIST has delegated the authority to the Department of Defense (DOD) to structure and assign values for code 6. The DOD must register the DSP structure for IDI code 6 with the NIST. Values for the DSP for IDI code 5 shall be assigned as follows in figure 18.

The NIST will assign the first two octets, which identify a government Organization, such as an agency, bureau or commission. The NIST will delegate to the organization the authority to further allocate and assign values for the remaining octets of the DSP.

The two-octet Subnet ID uniquely identifies a subnetwork within the organization's subdomain. The End System ID is intended to permit subnetwork administrators to specify information needed to deliver a message to an end system on the subnetwork. The format, value, structure and meaning of the End System ID is left to the discretion of the subnetwork administrator. The End System ID might be a physical address (i.e., subnetwork point of attachment (SNPA) address) or a logical address, with or without structure.

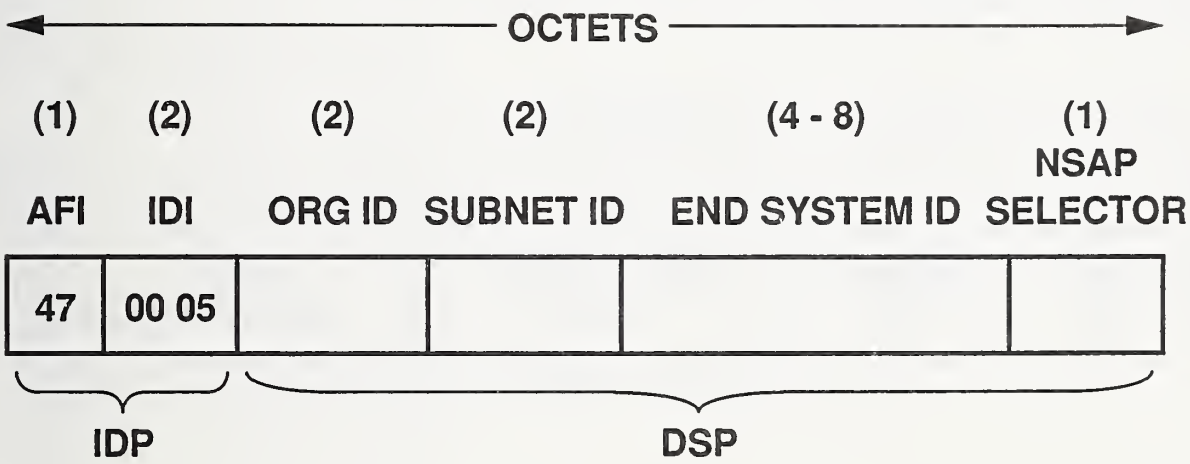


FIGURE 17
U.S. GOVERNMENT NSAP
ADDRESS STRUCTURE

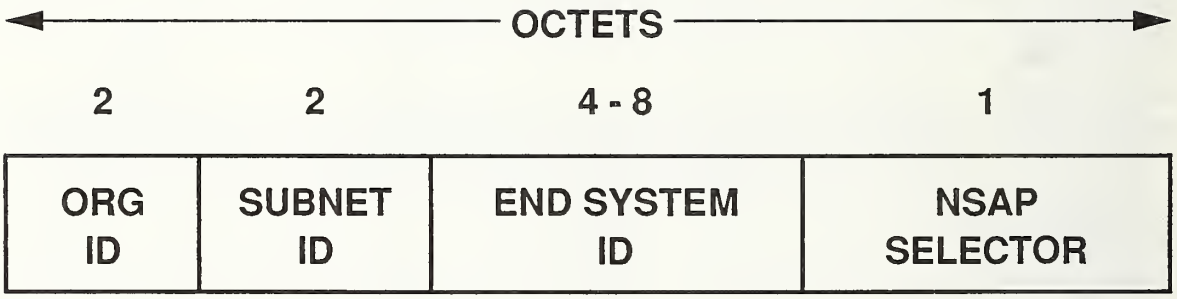


FIGURE 18
DSP ALLOCATION

The NSAP selector identifies a Transport entity. The NSAP selector may also identify other direct users of the Network service if required by the acquisition authority. The NSAP selector is one octet in length, represented in binary. The value 1 identifying the ISO Transport Protocol entity is recommended for both codes 5 and 6. The end system administrator may choose to assign different NSAP selector values and, therefore, the GOSIP allows configurable NSAP selector-to-Transport layer mappings because, for example, several Transport entities may co-exist in some systems.

Many Federal agencies will be routing information entirely within the civilian sector or entirely within the military sector; some will be routing between civilian and military, or vice versa. In the former case both the AFI and IDI fields add no value to routing data.

The Organization ID identifies a unique organization within a domain. For example, the Department of Transportation may be registered as an organization in the U.S. Government domain. There are two octets (16 bits-binary) assigned for this space. Each U.S. Government agency must apply to the NIST (or to the DOD under IDI code 6) in order to get a unique identifier assigned, using procedures described in section 8.3.3.

The remaining octets of the DSP specify components within a major Government organization. These values are assigned by elements within the particular agencies. The Subnet ID specifies a particular subnetwork identifier. There may be many subnetworks within an organization, and each will get a unique identification. Information will be routed within a particular organization towards a particular subnetwork until that desired subnetwork is found.

Once the subnetwork is found, routing occurs within that subnetwork to find a particular end system; this is done by specification of the End System ID field. The value of this field may be a physical address (SNPA) or a logical value; in the latter case a locally administered table will be used to map the logical address to a corresponding physical address. Once the end system is found, the directional routing stops; now all that remains is to find the appropriate user of the network layer service within that end system; this is done by examining the value of the NSAP selector field. The complete routing process is illustrated in the example below.

EXAMPLE: An agency system receives the following NSAP:

47 00 05 00 32 12 34 53 18 44 27 01

This NSAP will be interpreted as follows: 47 is the AFI, 00 05 is the IDI, 00 32 is the Organization ID, 12 34 is the Subnet ID, 53 18 44 27 is the End System ID, and 01 is the NSAP selector.

8.3.3 Detailed Registration Procedures

The steps required to register an NSAP organization ID are given below.

1. Establish that OSI communication will take place intraagency or interagency (e.g., that a need for registration exists).

2. Identify all end systems, intermediate systems, subnetworks, and their relationships.

3. Designate one individual (usually the agency head) within an agency to authorize all registration requests from that agency (NOTE: All agency requests must pass through this individual).

4. Send a letter (on agency letterhead and signed by the agency head) to Group Leader (ORG ID), Program Coordination and Support, National Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899. This letter must include at a minimum the following: name and address of organization, phone number of organization, suggested Organization Name, and date needed.

The Organization Name must be no more than 64 ASCII characters. The appropriate form in Appendix C should accompany this letter.

5. The NIST will convert the Organization Name to an NSAP Organization ID, and retain these values in its documentation. There is a one-to-one correspondence between Organzation Name and NSAP Organization ID. If the Organization Name is a duplicate of one previously received or has an invalid length or format, the request will be rejected.

6. If accepted, the NIST will send a return letter to the agency head indicating the NSAP Organization ID assigned, Organization Name registered, effective date of registration, and any other pertinent information.

7. If rejected, the NIST will send a letter to the agency head explaining the reason for rejection and requesting alternate assignments.

8. Each agency will assign and register its own subaddress space in accordance with the procedures set forth by the NIST in section 8.3.4.

9. The NIST will maintain, publicize, and/or disseminate the assigned values of Organization IDs unless specifically requested by an agency not to do so.

8.3.4 Guidelines for NSAP Assignment

Recommendations which should be followed by Federal users in making NSAP address assignments are given below.

(1) The agency should determine the degree of structure of the DSP under its control. Further delegation of address assignment authority (resulting in additional levels of hierarchy in the NSAP address) may be desired.

(2) The agency should make sure that portions of NSAP addresses that it specifies are unique, current and accurate.

(3) The agency should ensure that procedures exist for disseminating NSAP addresses to organizational units within the agency.

(4) The systems administrator must determine whether a logical or a physical address should be used to identify the end system. Logical addressing may be used when flexibility in assignment of system addresses is desired; otherwise, it is recommended that physical addresses (e.g., SNPAs) be assigned for simplicity and convenience.

(5) For the NSAP selector, it is recommended that integer values of between 56 and 255 be used to identify users of the Network service other than the Transport service. It is also recommended that values be assigned downward from 255 whenever possible.

(6) The components of the NSAP required for routing must be maintained and updated at each intermediate system.

(7) End systems and intermediate systems in Federal agencies must be capable of routing information correctly to and from non-GOSIP systems (NOTE: This is true when the AFI equals 47 but the IDI is not equal to 5 or 6, or the AFI is not equal to 47).

(8) The Organization Name will also serve as the MHS Organization Name for MHS implementations (see sec. 8.4.3).

(9) An agency may request the assignment of more than one Organization ID. A justification should

accompany such a request. Such requests will only be approved if the justification is sufficiently strong.

(10) The End System ID value assigned should not depend on the originator of the packet or on the routing used to reach that end system.

8.3.5 Transport Service Access Point (TSAP) Selector

A TSAP selector identifies a point within an ADP system where information is passed between the Transport Layer and the Session Layer (in both directions). The TSAP selector does not have to be unique globally, but must be unique within an end system; it is appended to the NSAP address to identify a user of the Transport service. There may be more than one TSAP selector per end system; each identifies a separate user of the Transport service.

The TSAP selector has meaning only within an end system. The GOSIP FIPS identifies a value of 1 (to identify OSI Session) for convenience. Other values (2,3..) may be assigned to identify different users of the Transport service. Other values can be assigned for the TSAP as long as they are the correct type and format (see sec. 5.2 of the GOSIP FIPS), and are interpretable by the destination end system. If a particular TSAP selector of one end system must be known to another end system, that value could be conveyed a priori or by a common directory service.

8.3.6 Session Service Access Point (SSAP) Selector

The SSAP selector identifies a point in the system through which information passes in both directions between the Session Layer implementation and the Presentation Layer implementation (see sec. 7). The SSAP selector identifies a user of the Session service. The GOSIP FIPS recommends a value of 1 to identify the Presentation Layer and 2 to identify MHS; other values would identify other users of the Session service. There may be more than one SSAP selector per end system; each would identify a different user of the Session service.

Any value may be inserted for the SSAP selector as long as it is the correct type and format (see sec. 5.2 of the GOSIP FIPS), and is correctly interpretable at the other end system. In transmitting information the SSAP selector is appended to the end of the TSAP address. If it is necessary for one end system to know the SSAP selector for another end system, then that information could be conveyed a priori or via a common directory service.

8.3.7 Presentation Service Access Point (PSAP) Selector

The PSAP selector identifies a user of the Presentation service in an end system. The PSAP selector does not have to be globally unique. As described in the GOSIP FIPS, the PSAP selector is actually encoded as an octet string or as an integer; a value of 1 is recommended for FTAM. There may be more than one PSAP selector per end system; each value identifies a different user of the Presentation service. Several different applications on an end system may be bound to a particular PSAP selector.

Any value may be inserted for the PSAP selector as long as it is the correct type and format (see sec. 5.2 of the GOSIP FIPS), and is correctly interpretable at the other end system. If it is necessary to identify a PSAP selector on one end system to another end system, a common directory service could be used, as well as an a priori method.

A PSAP address consists of the PSAP selector appended to the SSAP address, and is intended to globally identify an application. For ICD 5, as an interim measure, until directory services are available, agencies that wish to communicate with OSI end systems administered by different registration authorities may register their complete PSAP addresses with the NIST.

To perform this registration, users should send a tar-formatted file containing the entries to the NIST using the address below. The NIST will move the entries into a directory, under the filename "orgid.psaps."

Users may access this directory electronically using a userid and password that will be sent upon receipt of the entry information. The address for correspondence is: Chief (ATTN: PSAP Registration), Systems and Network Architecture Division, National Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899.

8.4 Application-Specific Registration Objects

The second group of objects to register for the GOSIP FIPS is as follows: (1) FTAM document type names, (2) MHS private body parts, and (3) MHS Organization Names. FTAM document type and MHS private message body registration is optional and should only be requested under special circumstances. MHS Organization Name registration is required for all MHS implementations.

8.4.1 FTAM Document Type Name

Document types in FTAM are simple descriptors of the structure, syntax, and semantics of a file. This information is separate from the file contents itself; it tells how the records and blocks of data that constitute a file are organized, as well as how long each record or block is, and the range of data types that are possible in the file contents. For example, a file could be a single binary file of length 10000 bits, or it could be a sequence of 200 fixed-length records of 50 ASCII characters each, with CR (carriage return) and LF (line feed) symbols separating the records. Each of these is a different document type, and so has a different document type name.

This document type information must be passed between two systems using the FTAM protocol, to enable each system to properly anticipate what will be transferred and to accommodate the data when it is transferred. Thus it is important to register document type names.

There are standard "registered" document types of the kind described above that exist. Some are defined in the ISO FTAM International Standard and some are defined in the NIST Workshop Agreements. These generic document types have been defined because they represent file structures that are universally used and easily described.

Agencies may have unique file structures that do not conveniently fit into any of these defined document types. If agencies plan OSI communication with other agencies using these unique file descriptors, then they should be registered with the NIST using agency-defined document type names. If communication is within an agency, then registration with the NIST is not necessary, but procedures should be in place within that agency to make sure that the document type information is understood and interpreted correctly.

The pre-existing document types should be used by agencies whenever possible; it is anticipated that these will cover most file types of interest to Federal agencies. An agency should (1) examine these pre-existing document type names for suitability and (2) if additional document types are needed, and OSI communication is required with another agency, then the agency head may apply to the NIST for a registered document type name, using the procedures given in section 8.4.4 and the appropriate form in Appendix C.

8.4.2 Private Message Body Parts

A message body part number describes the form and syntax of the data being transferred. All MHS implementations are required to generate IA5 (ASCII) text. MHS vendors will specify if additional body part types are supported by their implementations.

The CCITT X.400 Recommendations Series defines 12 generic body part types. It is anticipated that these pre-defined body part types mentioned above will satisfy Federal requirements for transferring MHS information. In exceptional instances, Federal agencies may require the assignment of special body part numbers to communicate special messages to other agencies.

An agency must register private body part descriptors with the NIST as described in section 8.4.4, under

the following conditions: (1) the agency has special body part requirements which cannot be satisfied by any previously-defined body parts, and (2) MHS communication will occur with other agencies. The appropriate form given in Appendix C should be used. If all MHS communication is within an agency, then registration with the NIST is not necessary; however, agencies should ensure that procedures exist to correctly define and interpret private body part information. The NIST will return the number corresponding to the private message body part descriptor. Procedures for using this number are given in section 7.5.3.6.2 of the NIST Workshop Agreements [NIST 1].

8.4.3 MHS Organization Names

MHS originators and recipients are identified by means of a parameter called the Originator/Recipient Name (O/R Name). The O/R Name is encoded as a set of attributes. GOSIP requires that five of these attributes be supported by MHS implementations (see the GOSIP FIPS, sec. 5.3.2 [NIST 2]) including the Organization Name. The Organization Name of an agency is automatically registered when an agency requests an NSAP address (see sec. 8.3.3).

The NIST delegates to the organization indicated in the Organization Name the authority to assign Organizational Units and Personal Name attributes for that agency. Typically, a personal name is a surname or a surname followed by a given name, but it can also identify a role within the organization (e.g., President) or an office within the Organizational Unit.

Assignment of the Organizational Unit attribute values is optional; i.e., MHS users can be identified by Organizational Name and Personal Name only. The agency Address Registration Authority must ensure that no duplication occurs in the attribute assignments. The Organizational Unit and Personal Name attribute values are not registered with the NIST.

8.4.4 Procedures for Registration

The following procedures should be used now and in the future to register FTAM document types and/or MHS body part names:

(1) determine that special FTAM document types and/or MHS body part names are necessary in inter-agency OSI communication (NOTE: This may be done by examination of currently registered descriptors),

(2) designate one official within each agency (preferably an agency head) authorized to rule on these registration matters,

(3) mail the appropriate form given in Appendix C to: Group Leader (FTAM or X.400, as appropriate), Program Coordination and Support, National Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899, and

(4) the NIST will act on each request (NOTE: If the request is rejected, the reason for the rejection will be returned.)

8.5 Future Registration Objects

Additional protocols will be included in future versions of the GOSIP. The protocols may require the registration of additional information. When the information is generic, registration will most often be done by the developers of the standard or the vendors that implement the standard. When the information is specific to the needs of a closed community, registration will be the responsibility of the user. Some examples of objects that may require registration follow.

Presentation contexts are standard representations of abstract syntax definition-transfer syntax pairs between cooperating entities or individuals. Two organizations, for example, would reference a standard descriptor of information transfer format that both sides would understand. This descriptor is called a

Presentation context. Commonly-used contexts will in all likelihood be registered. See section 7.3.4 for more information on the Presentation Layer. An example of a Presentation context would be "FTAM ASN.1 description encoded using ASN.1 basic encoding rules"; in this example ASN.1 refers to "abstract syntax notation one."

Application context names describe the Application processes that communicate in an OSI environment. Some generic names (corresponding to OSI applications) are likely to be registered in the future. An example of application context might be "FTAM used in combination with ACSE."

Document Application Profiles (DAPs) are being developed for the Office Document Architecture (ODA) standard. These DAPs will describe the document formats that are transferred.

Implementation of the Virtual Terminal standard may require the registration of terminal profiles and control objects. A terminal profile is a complete and consistent set of parameters relating to a particular type of terminal (e.g., TELNET). Control objects are used to transfer terminal information that refers to "value added" features that are specific to a terminal type. An example is a control object which provides a sophisticated coloring capability for graphic terminals.

FTAM constraint sets are sets of possible file structures which may be applied against the general FTAM hierarchical file model (see sec. 7.3.2 and Appendix A) to limit the options available to users. Constraint set names give basic structuring information only, and are not as comprehensive or as specific as FTAM document types. An example of a constraint set would be the set of all sequential record-oriented files. See the FTAM standard for a complete list of predefined constraint sets. It is likely that these generic constraint sets will be officially registered in the near future.

Relative Distinguished Names identify directory entries; there is a one-to-one correspondence between these names and directory entries. These Relative Distinguished Names for the GOSIP will include Organization Names, and a hierarchy of names comprises a unique identification.

A directory enables users to identify, understand, and locate objects within the network. These actions are accomplished through names, attributes, and addresses, respectively. The user supplies to the directory service a Relative Distinguished Name. The directory service returns a set of attributes corresponding to the name. It is anticipated that the Organization Name allocated with the NSAP will be a first-level key component of GOSIP Relative Distinguished Names.

8.6 Other General Registration Issues

The general registration guidelines below should be followed by agency representatives, in all of the registration situations discussed previously.

(1) Once a value is assigned to an agency by the NIST or the DOD, that value may not be used in any other context, and it may not be changed subsequent to that assignment without authorization of the assigning registration authority.

(2) Agencies should develop policies to coordinate the assignment of values to objects which ensure consistency and uniqueness.

(3) Upon written request, the NIST will disseminate a list of the specified registered objects; there may be a charge for this service. Inquiries may be addressed to: Group Leader, Program Coordination and Support, National Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899.

(4) A registration subauthority within an agency must decide how much (if any) control to delegate to further subauthorities within that agency to register objects.

(5) The NIST will assign only one value at a time per specific request; separate forms must be submitted for each specific value request. A justification must be included as to why a value is necessary. The NIST will not "reserve" a block of values for agency use. Each request will be considered on its own merits.

(6) Technical individuals knowledgeable in OSI communications should be the points of contact for all OSI registration issues in each agency.

(7) Any of the following reasons may be used by the NIST to reject a registration request: (1) incomplete or incomprehensible definition, (2) existence of an identical entry elsewhere, (3) nonconformance with standard practices, or (4) inadequate justification for inclusion.

(8) It is recommended that agencies keep specific registration requests to a minimum, and do not request more values than are necessary.

8.7 Summary

In summary, for the GOSIP FIPS, the OSI objects to register are the NSAP Organization ID, FTAM document type name (optional), MHS Organization Name, and MHS private body part (optional). It is important to register these objects in order to provide unique identification for OSI communication in a Government-wide environment.

In order to register an NSAP Organization ID, users should follow the procedures given in section 8.3.3, using the appropriate form in Appendix C. An Organization Name is submitted, and this Organization Name will be converted by the NIST into an NSAP Organization ID. There is a one-to-one correspondence between the NSAP Organization ID and a given Organization Name. The Organization Name will also be registered by the NIST for use in MHS implementations as an MHS Organization Name. The Organization Name will serve in the future as a key component of a directory Relative Distinguished Name.

In order to register FTAM document types and/or MHS private body parts, after a determination that predefined values will not suffice, procedures given in section 8.4.3 should be followed. The appropriate form in Appendix C should be used for this purpose.

Section 8.5 gives an indication of likely registration issues for future versions of the GOSIP. Agency officials should read and understand this information, as well as the guidelines given in section 8.6. Registration information is also found in section 5 of the GOSIP FIPS [NIST 2].

9.0 GOSIP TRANSITION STRATEGIES

9.1 Introduction

GOSIP creates an opportunity for each Federal agency to assert control over future procurement. Adoption of GOSIP as a long-term strategic initiative will lead to evolution of current systems into a GOSIP-compliant interoperable set of computers within that agency. What follows is some general advice concerning a transition towards GOSIP-based networks, which will provide the benefits to agencies that have been previously described.

In this section, recommendations for transition strategies will be given and specific alternatives will be proposed based upon an agency's particular requirements. It should be emphasized that the information in this section is only a recommendation. It is up to the procurement and technical authorities in each office to make the proper decisions on transition based upon their own particular situation.

Each of the subsections below offer a different perspective on the OSI transition problem. Agencies may want to adopt more than one solution for different components of ADP systems. A higher level of integration will then take place combining each of these proposed solutions. The end result is a GOSIP-based internetwork. As current systems reach the end of their life cycles, they should be replaced by GOSIP-compliant systems.

Section 9.2 gives a generic course of action for Federal agencies in transitioning to GOSIP systems. Agencies may currently find that one of two possibilities exists as follows: (1) current architectures map conveniently into the OSI architecture, and (2) there is no convenient mapping between current architectures and OSI architectures. These two possibilites will lead Federal agencies to different courses of action.

When the architectures map conveniently, suggested strategies to follow are described in section 9.3. Section 9.4 elaborates on actions when the architectures do not map. Section 9.5 describes strategies for interoperability with non-GOSIP OSI systems. General considerations for transitioning to OSI systems are given in section 9.6, and finally, a brief summary follows in section 9.7.

In transition to GOSIP systems, a comprehensive transition plan must be devised as soon as possible, and policy makers within an agency should coordinate acquisitions to take account of all of the factors that are important to correctly assimilate OSI technology into the Federal environment. Vendors and users should discuss how these strategies will be implemented in particular situations.

9.2 Perspective on the Process

The single most important recommendation for an agency is that a clear and definitive policy be established concerning the adoption of GOSIP. Such a policy serves several goals. First, a clear and definite signal is sent to agency operating components that a future networking direction has been set. The operating units can then begin to plan seriously for transition, knowing that agency backing is assured. Network suppliers are also put on notice that the agency is going in the direction of GOSIP. These vendors can then reorient their marketing strategies accordingly.

Having announced a clear policy, an agency should require that each affected operating unit prepare a transition plan indicating the time goal and mechanisms for implementing the policy. Intelligent planning for, and adoption of GOSIP will pay dollar benefits over the long term. However, it is unrealistic to expect an operating unit to adopt the provisions of GOSIP at an inappropriate point in the life cycle of its systems. Adoption of GOSIP should be coordinated with plans for replacing or upgrading major computer and network systems.

Once a transition plan is in place, orderly implementation of interoperable computer networks can begin. Implementation will involve the procurement process, the network design process, and education of users and consultants within the agency. This strategy is being successfully applied by the DOD to implement

OSI, and it is likely that it can be successfully applied by other agencies as well.

An agency should (1) examine where it is now with respect to OSI technology, (2) determine where it wants to go, and (3) determine how to get there (i.e., via a series of steps or stages). Each alternative should be examined to determine what is most appropriate for that agency. Following this, a decision should be made on which strategy is best, and the appropriate recommendations should be made and implemented in acquisition plans. Agency policy with respect to life cycle management must be integrated into these decisions (e.g., duration of the cycle, components of the cycle). Resource materials on OSI (including this Guide) should be extensively consulted.

Given that an agency has vendor-specific configurations, several decisions must be made as follows: (1) an agency must develop a procurement strategy in accordance with the instructions in section 6 and (2) an agency may consider applicability and waiver procedures (as described in sec. 5).

Vendors will make suggestions as to how to provide a smooth transition to OSI while preserving capabilities inherent in their particular user interface during the OSI transition process. The vendor whose architecture differs radically from OSI is likely to emphasize the private architecture approach while offering gateways to OSI products. On the other hand, the vendor whose private architecture is close to that of OSI is more likely to effect a smooth transition to a total OSI solution; in this case, private architecture solutions will have a limited life. For more on gateways, see section 9.3.

9.3 The DOD Approach

The Department of Defense (DOD) has taken a leading role in the evolution of networking. The Defense Advanced Research Projects Agency (DARPA) has been instrumental in network research. There are two major networks that compose the Defense Data Network (DDN): ARPANET, which is a research and development network, and MILNET, which is an operational communications network

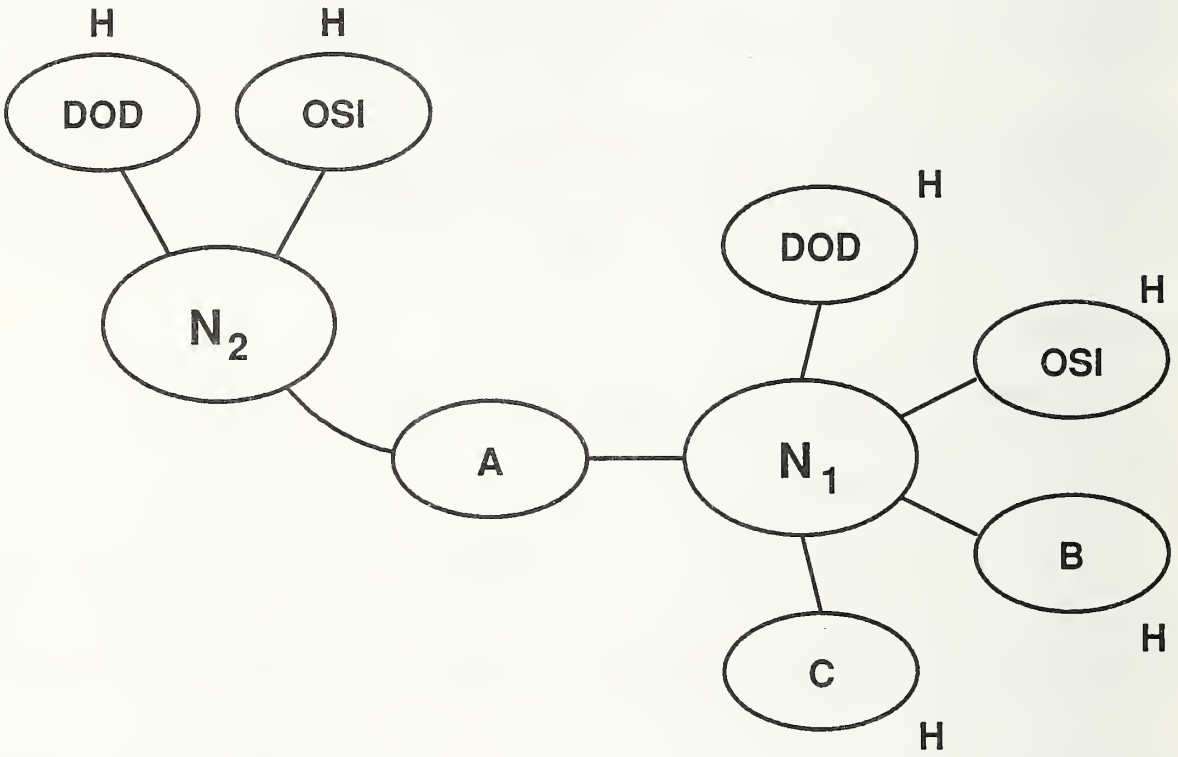
The DOD issued a three-page policy statement in July 1987 announcing plans to adopt the GOSIP FIPS and to begin transition of the DDN to GOSIP protocols. In June 1988 the DOD issued a plan for implementing the policy. Several independent agencies of the DOD are procuring GOSIP products to gain operational experience. Other components are permitting vendors to offer either GOSIP or DOD protocols. The DDN backbone plans to move toward complete use of the GOSIP protocols by 1993.

There are many environments in the Federal Government (civilian and military) that use the MILNET, the ARPANET and other interconnected networks. The DOD has investigated OSI transition and interoperability issues extensively and the approaches taken by the DOD are deliberately generic. Accordingly, any of the DOD approaches to transition may be used in other situations and in other environments, particularly where there is a functional equivalence between existing architectures and the OSI architecture. In 1990, the OSI protocols will become the sole mandatory interoperable protocol suite for new DOD acquisitions; however, a capability for interoperation with DOD protocols must be provided for the expected life of systems supporting the existing DOD protocols.

The DOD approach to transition is multi-faceted, including: (1) developing a full stack of OSI protocols in a portable operating system environment (ISODE and POSIX (for both, see sec. 9.3.1)), (2) having both protocols co-exist on a particular host (dual-protocol host), (3) converting from one Application-Layer protocol to another (Application Layer gateway), and (4) supporting both DOD IP (Internetwork Protocol) and CLNP at the Network Layer (dual IP gateways); each of these has advantages and disadvantages, and all may have particular importance in a variety of situations. An example internetwork scenario showing some of these methods is given in figure 19.

9.3.1 ISODE and POSIX

The DOD protocol stack and the OSI protocol stack are functionally similar; therefore, it is possible to build a protocol implementation with a mixture of DOD and OSI protocols in the stack ("mixed" stack).



A = DUAL IP GATEWAYS
B = APPLICATION - LAYER GATEWAYS
C = DUAL - PROTOCOL HOSTS
H = HOST
N_n = NETWORK $_n$

FIGURE 19
DOD TRANSITION APPROACHES

The ISODE (ISO Develpment Environment) is a UNIX-based public domain software package that includes the OSI Application, Presentation and Session Layers. The ISODE runs over the OSI lower layers, but it also contains an interface which allows the OSI upper layers to "run" over the TCP (Transmission Control Protocol). Using this interface, OSI applications can run in a DOD networking environment using DOD hosts. The disadvantage of this approach is that an end system can communicate only with end systems that have the same mixed protocol stack; however, this alternative may be useful as a research or education tool during the transition period.

POSIX (Portable Operating System for Computer Environments) is a standard application interface for UNIX-like operating systems. Efforts are underway to put additional functionality into ISODE and to make ISODE POSIX-compliant.

The National Institute of Standards and Technology, the University of California at Berkeley, the University of Wisconsin at Madison, the Wollongong Group, the MITRE Corporation and the University College of London are working together to produce an implementation of the OSI protocols running on a POSIX-conformant version of the Berkeley UNIX operating system. ISODE will be augmented to provide the GOSIP protocol profile for layers 5 through 7 in a POSIX environment. This will permit DOD hosts to be replaced by OSI hosts without changing the operating systems environment. IBM has donated the Class 4 Transport and CLNP Kernel code for this project.

The goal of this project is to disseminate an implementation of the OSI protocols to the academic and research communities that use Berkeley UNIX. In addition, the ISODE software could serve as a reference implementation for GOSIP interoperability testing. With POSIX-conformant OSI protocols, as well as anticipated POSIX extensions to define an interface for network services, OSI products could be much more portable.

9.3.2 DOD-OSI Dual IP Gateways

In order for DOD-OSI internetworking to occur, it is necessary to provide for OSI hosts on a local area or wide area network the ability to communicate with other OSI hosts on another DOD-based local area or wide area network. Since the DOD IP and OSI CLNP are similar in functionality and protocol structure, dual gateways are a viable alternative. The availability of dual IP gateways would reduce the number of components, and therefore presumably reduce the cost and complexity for DOD LANs that are composed of a mixture of DOD and OSI protocol hosts, allowing the use of DOD protocols in areas in which OSI protocols are not yet mature (e.g., internetwork routing and network management).

In either the DOD or OSI protocol architectures, the Internet Protocol (IP) or CLNP performs the address translation and routing functions required to connect nodes on the same network or different networks. A DOD/OSI IP gateway is a device that will be able to distinguish between the DOD and OSI internetwork protocol data units When a packet arrives at an intermediate system, a network layer protocol identification field is checked and then the packet is passed to the appropriate module (either DOD IP or OSI CLNP).

9.3.3 Dual Protocol Hosts

A dual DOD protocol host has the complete OSI and DOD protocol suites available as part of its networking capabilities. A user of such a host would have the option of invoking the DOD protocols (TELNET for remote login, FTP (File Transfer Protocol) for file transfer, and SMTP (Simple Mail Transfer Protocol) for electronic mail) or the analogous OSI application protocols (VTP for remote login, FTAM for file transfer, and MHS for electronic mail).

A dual protocol host can be used directly by users with accounts on it to communicate to any OSI or DOD destination It can also be used as a staging point for manual interoperation between a host that has only DOD protocols and a host that has only OSI protocols. A user on a host that has only DOD protocols could transfer a file to a host that has only OSI protocols by using a dual protocol host as an intermediary.

9.3.4 Application-Layer Gateways

An Application Layer gateway is a dual protocol host which contains a conversion module residing at the Application Layer of each protocol stack. This module performs the semantic, syntax, and service transformation required for the protocol conversion.

The OSI File Transfer (FTAM) and Message Handling (MHS) protocols (sec. 7) are candidates for such a gateway. The NIST has developed and tested prototypes of a gateway connecting the DOD SMTP and the OSI MHS protocols, and a gateway connecting the DOD FTP and OSI FTAM protocols. The NIST effort demonstrates the viability of a relatively efficient means of interoperation between systems based on the Transmission Control Protocol (TCP) and OSI-based systems.

The gateways were designed so that users require minimal knowledge of the remote protocol, as much capability as possible is retained for each protocol, and the protocols being converted are not modified. Figure 20 illustrates how the SMTP-MHS and the FTP-FTAM gateways would look schematically.

9.4 Other OSI Transition Concerns

The second class of existing architectures, as mentioned previously, do not map conveniently to the OSI architecture. The choice of alternatives to use represent implementation decisions that should be made by the vendors. Users should concentrate on stating their functional and performance requirements.

Users choose interoperability solutions based upon an understanding of end-user requirements; these requirements are evaluated on such factors as the level of interoperability required, the range of vendor(s) equipment to connect, the cost to implement and maintain, and the implementation schedule requirements. In addition, the degree of network management required and supported is a significant factor in providing reliable service to the end user.

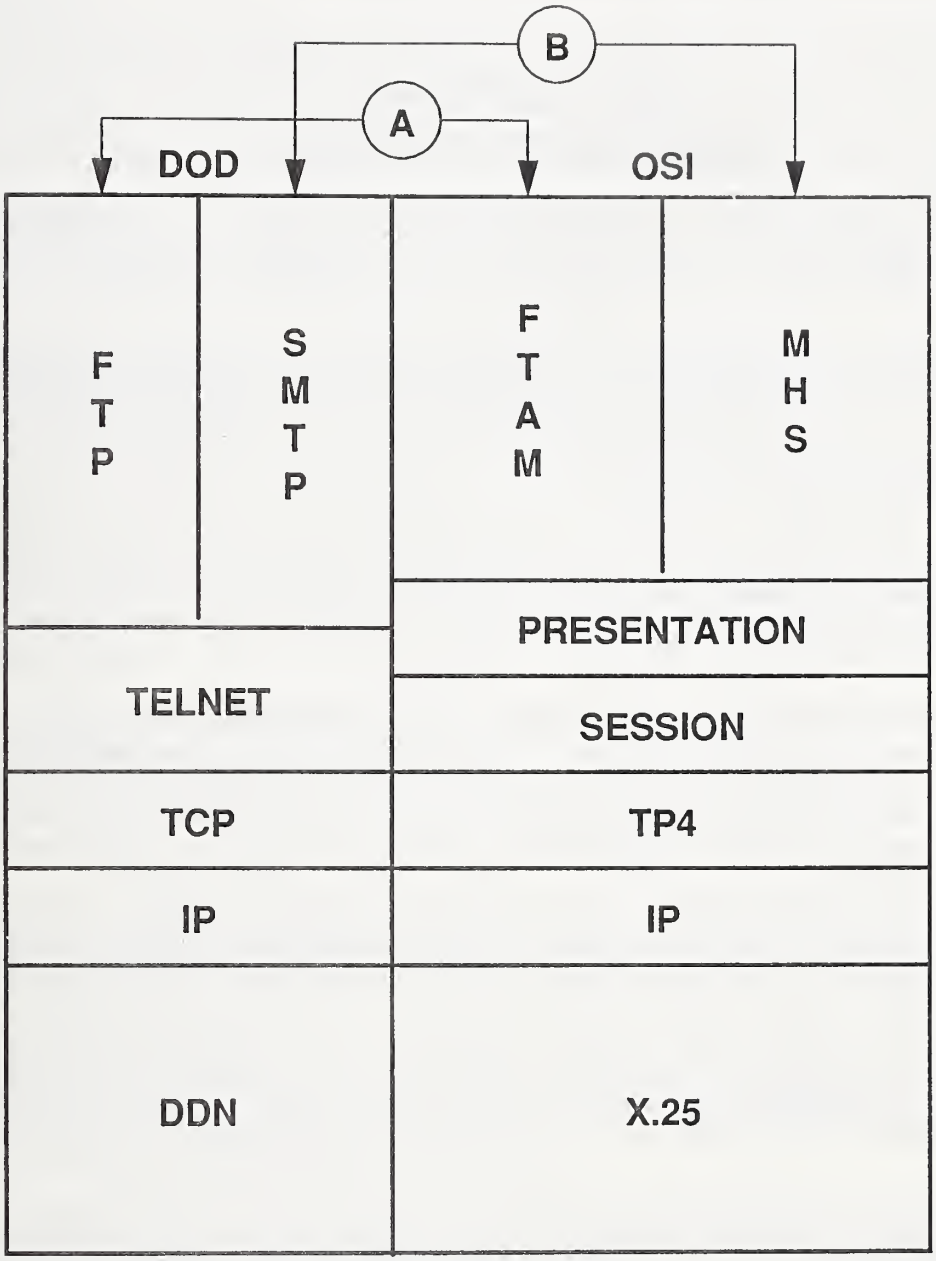
Other concerns for interoperability involve: (1) the sharing of hardware resources such as terminals and communication links, and (2) support for interoperation of a basic set of application functions. In addition, there is the need for application-to-application interoperation.

The most comprehensive and simplest interoperability is achieved by implementation of equipment conforming to a single full-function networking architecture. For environments involving multiple vendor architectures, a compromise may exist between the level of interoperability achieved and the number of vendor environments to be supported.

Terminal protocol converters or emulators provide an inexpensive and effective interoperability capability for single architecture networking environments. Gateways may be optimized for performance but are difficult to extend to support additional vendors' environments.

Gateways may be the best approach for interoperability between products of a small number of vendors (two or three). International standards provide the most appropriate approach for interoperability between a large number of different vendors.

Vendors whose architectures do not map conveniently to the OSI architecture may decide to provide gateways or protocol converters as a long-term solution, while (a) providing for a gradual transition to OSI, or (2) allowing both OSI and the existing native architecture to co-exist permanently. It is possible that special user services which exist in the native architecture will be preserved by the vendor; OSI will be available via special hosts or processors. As another approach OSI could be used to permanently interconnect two native architectures. Users should transmit to vendors any critical requirements in these areas, and allow vendors to develop specific responses to these concerns.



A = FTAM - FTP GATEWAY
B = MHS - SMTP GATEWAY

FIGURE 20
GATEWAY ARCHITECTURAL MODEL

9.5 Interoperability With Non-GOSIP OSI Systems

A problem that Federal agency systems administrators must consider is that of communication with non-GOSIP OSI systems. This is primarily because many non-GOSIP systems use the CONS (Connection-Oriented Network Service) and Transport classes other than Class 4, whereas GOSIP-compliant systems are linked by the CLNP (Connectionless Network Protocol) and Transport Class 4. To effect the required interworking, Federal agencies must employ procedures outside the scope of GOSIP.

There have been several interim measures proposed to handle this incompatibility, including: (1) a "265" interworking function, (2) a DSG (distributed systems gateway), (3) a MSDSG (multi-system DSG), and (4) an Application-Layer gateway. All have some disadvantages and advantages.

The "265" interworking solution is a Network relay that uses the connection-oriented and connectionless network services to forward data to Transport Class 4 processes. Since Transport Class 4 must be used at both ends of the Transport connection, this solution has little support in the connection-oriented community, which typically uses Transport Class 0 or 2.

In the DSG approach, a Transport Layer relay is used to provide the inter-working between connection-oriented and connectionless end systems. This approach is viewed by some to be a violation of the OSI architecture, which expressly forbids Transport Layer relays. This approach is viewed by others to conform by considering the connection-oriented environment as a single large OSI system when viewed from the connectionless environment and vice versa.

The MSDSG approach is a variation of the DSG which simplifies NSAP addressing. Neither the DSG or MSDSG approach places any restrictions on the class of Transport that is used by GOSIP and non-GOSIP OSI systems. Since the same class of Transport cannot be assumed, end-to-end security mechanisms that rely on a particular class of Transport or hop-by-hop security relying on the CLNP cannot be assured. None of these three approaches has been widely implemented. Users should consult with their vendors for additional security information.

In contrast to the other three approaches, the Application Layer gateway is architecturally correct and is particularly useful in the relaying of messages between Message Transfer Agents which use Transport Class 0 and the CONS, and those which use Transport Class 4 and the CLNP. (See Appendix A for additional information.) In addition, implementations of the Application-Layer gateway for this purpose (relay MTAs) are expected to be widespread. The Application-Layer gateway can also be used to implement security services at the Application Layer. For applications such as file transfer, virtual terminal, and transaction processing, Application-Layer gateways introduce inefficiencies that would not normally exist.

The choice means of assuring interoperability across CLNP, CONS, and the most common range of Transport classes is purchase of end systems capable of supporting all the required services. Many vendors serving the international marketplace offer Transport Classes 0,2, and 4 and also offer both CLNP and CONS. This solution will work well when an end system is connected directly to a wide-area network supporting CONS. When end systems are attached to a local area network, where CONS is usually not supported, interworking solutions such as "265", DSG, MSDSG, and Application-Layer gateways become more important

9.6 General Transition Issues

The following general guidelines will serve to further assist users in making decisions relating to OSI, and in properly implementing the decisions that are made. These considerations apply to all of the information previously discussed, and are independent of any particular strategy selected. It is important for vendors and users to work out mutually acceptable agreements regarding a particular agency and OSI. Users should give any functional and configuration requirements, and vendors should attempt to suggest and design optimal specific solutions for particular user concerns.

Considerations are divided into the following categories: general (architectural), and user-related. These are presented below.

GENERAL (ARCHITECTURAL) ISSUES

These issues deal specifically with configuration or architectural considerations.

(1) Some questions are : (a) will the vendor migrate to OSI from its native environment?, (b) will compatibility between phases be maintained?, and (c) will gateways play a role in the vendor's long-term strategy?

(2) Other questions are: (a) does the vendor have an OSI migration plan for customers?, (b) can existing applications be protected in the transition to OSI?, and (c) can both proprietary and OSI protocols be supported in initial OSI offerings (e.g., in all products or just selected ones)?

(3) It is important to determine if communications between an OSI product and a proprietary product will be supported, and if previous releases of the vendor's proprietary network products will work with new OSI releases.

(4) The vendor should have an OSI migration plan for customers. Where possible, compatibility between phases should be maintained. The schedule for the availability of OSI products within the context of the transition should be given.

(5) Are user interfaces to the network the same for both OSI and proprietary products, or are there different interfaces for each category?

(6) It is primarily a vendor choice as to whether an OSI implementation can be integrated with their user interface.

(7) There may be a number of proprietary functions that are not provided by OSI systems. There could be a slight loss of functionality if mapping between vendor proprietary systems and OSI systems occurs. Users should be conscious that some loss of application functionality may occur with introduction of OSI products.

(8) How will access be supported to wide area networks? Will both OSI and proprietary networks use (a) X.25 packet switching, (b) X.21 circuit switching, (c) leased lines point-to-point, and (d) ISDN? How will access be achieved (host directly connected to wide-area network or intermediate system)? See Section 7 for additional information on these above-mentioned topics.

(9) If a vendor is making the transition from a proprietary protocol stack to OSI, the layer at which the conversion takes place may vary. In the transition, conversions could be performed at the link layer (bridge), network layer (intermediate system), and application layer (gateway).

(10) A vendor could migrate to OSI and abandon proprietary products, or maintain both OSI and proprietary products. OSI capability could exist across all product lines, or just a subset (hardware and software); also OSI capability may exist on all systems or just selected nodes.

(11) Will OSI-proprietary communication be transparent to user applications? Will this function be integrated with the operating system?

(12) Vendors should be encouraged to limit the number of embedded interfaces in hardware and software. This provides for flexibility in accommodating future enhanced OSI functionality.

(13) There is no requirement to provide OSI application software in all U.S. Government personal computers; there are other methods of making these services available to the end user. This does not

preclude vendors from offering and users from implementing OSI protocols within personal computers.

USER ISSUES

The suggestions described below deal with user issues in planning and developing a transition strategy. These issues should be discussed with vendors, but users have primary input.

(1) Cooperation of vendors should be solicited in developing a transition strategy; vendors can provide helpful suggestions as to how the move to OSI may best be achieved.

(2) Vendors should provide the same levels of functionality and service during a transition as before. Impact on user applications should be minimized.

(3) Not all Federal agencies need to communicate with other Federal agencies. Reasonable and prudent requirements for intra-agency and inter-agency interoperability should be determined and discussed with vendors.

(4) Not all transitions can be smooth. Short-term efficiency may need to be sacrificed for growth over the long term.

(5) It is important to keep subnetwork types consistent if possible, and to minimize the number of different kinds of networks involved in the transition. This will reduce the amount of work required to effect a transition.

(6) Modularize and isolate key network components in developing a transition plan. Identify the components that must be changed or procured.

(7) The practical impact on the network during upgrades should be considered (i.e., will all nodes be required to upgrade at the same time, and what will the total "down time" be?)

(8) An implementation task force should be appointed. This task force should be composed of individuals knowledgeable in the areas of the standards being referenced.

(9) A specific transition plan to OSI should be undertaken, with steps and dates included.

(10) It is important to keep future requirements in mind when planning a transition strategy. Such a strategy should allow for incorporation of additional OSI products when they become available.

(11) Multi-vendor product availability is an important reason to move toward GOSIP-compliant systems as quickly as possible even though usage may be restricted in the near future.

(12) In the near future, it may be necessary to specify nonstandard solutions to current concerns (e.g., network management) while striving for OSI standardization of these functions.

(13) Users should recognize that user and program interfaces to OSI services will likely be non standard into the foreseeable future; however, users should specify as much standardization as possible in procurement requests to maximize portability of people and applications.

(14) Users should recognize that the plan a vendor provides may be influenced by the degree to which the vendor's architecture differs from the OSI architecture.

9.7 Summary and Strategies

An agency may use any of the strategies defined above to move to OSI systems and may use combinations

of these strategies depending upon particular hardware and software configurations. These strategies are generic, and may be used to make the transition from any proprietary architecture to OSI. There are advantages and disadvantages to any particular strategy. These suggestions do not make an exhaustive list; there may be other approaches more suited to a particular agency's environment.

An agency should (1) examine long-term goals, (2) examine the advantages and disadvantages of each of the strategies given above, (3) determine which (if any) will be useful to an agency, (4) develop a specific transition plan based upon the strategies selected, and (5) develop an acquisition plan based upon the selected transition strategies. For large agencies, different strategies may be selected and it will be up to internal agency policy to coordinate the various transition strategies into an acceptable comprehensive transition strategy and acquisition plan. Factors to be considered in a transition strategy include cost, simplicity of implementation, and compatibility with current hardware and software design.

10.0 GOSIP CROSS-REFERENCE

10.1 Introduction

Developments are taking place in a number of different areas of computer standards which will help Federal agencies accomplish their missions more efficiently in the future. The GOSIP initiative, the subject of this Guide, is just one of a number of efforts aimed at reducing costs and increasing capability. In order for maximum effectiveness to be gained, it is important that the results be complementary. The ultimate goal is the integration of all of these separate areas into a vendor-independent standards-based architectural specification covering all pertinent aspects of computer and telecommunication systems for Federal Government procurement.

The NIST has defined an Applications Portability Profile (APP) to record a set of computer and communications standards that may be used to achieve data communications interoperability and software portability. The APP may lead to development of standard software interfaces across a range of computing services such as operating systems, networking, database, and graphics. The APP may benefit users by enabling standard software interfaces for computing and communications services to be referenced in future procurements. Figure 21 indicates the relationship of GOSIP to the APP effort.

Obviously, separate components of the APP should not conflict with each other in the final version. Still, while the profile is under development, it is important for Federal users to ensure that no inconsistencies exist when planning procurements relating to long-term ADP acquisition. In particular, GOSIP acquisitions and those involving other functional areas of the APP (such as database management, data interchange, and language development) should be examined for consistency at every stage of the procurement process.

The purposes of this section are to show how GOSIP fits in with the other programs, and to give guidance to Federal officials on strategies to pursue in integrating GOSIP requirements with requirements from these other efforts. It is important to require OSI products that will provide all of the capabilities necessary to support other efforts, particularly since OSI has so many optional features and services.

How can an agency best take advantage of these developments to fulfill its mission? The answer is that agency officials should (1) gain knowledge of each of the efforts described below (by consulting appropriate reference materials), (2) make a determination for each of these areas, whether or not this aspect of information technology fits with the agency's long-term ADP development strategy, and (3) if it does, then the agency should monitor the progress of each applicable program, and determine its impact, if any, on the work of their agency.

10.2 Interaction of Other Programs With GOSIP

Brief descriptions of programs affecting current and future Federal information processing procurement efforts are given below. The relationships of these programs with GOSIP are also discussed.

10.2.1 FTS-2000

FTS-2000 is a Government-wide upgrade of the Federal Telecommunications System (FTS) which is currently going through procurement. The General Services Administration (GSA) is administering this program. FTS-2000 will advance the communications capability of the U.S. Government, by replacing physical equipment, providing value-added services, and including digital capability. Voice, data, and video transmission will be supported over a variety of physical media, including those supporting ISDN and those supporting a packet-switched environment. The intent is to integrate these various means of transmission in an all-digital environment.

Close cooperation between GOSIP procurements and FTS-2000 procurements should be maintained. Communications requirements for FTS-2000 are functionally similar to those referenced by GOSIP when the requirements intersect (e.g., X.25 and X.400). When procuring GOSIP-compliant systems, U.S. Government

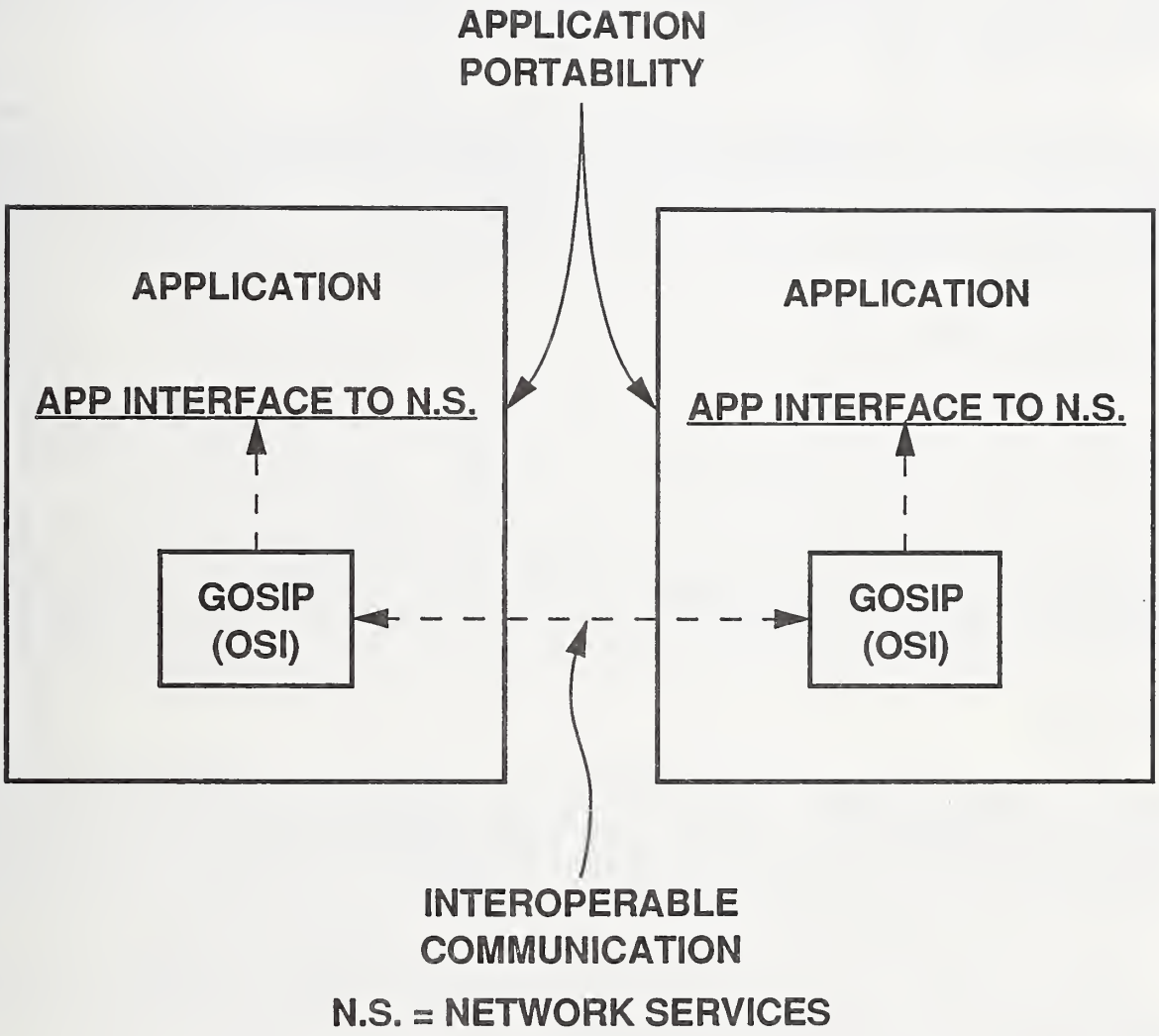


FIGURE 21
GOSIP AND THE APP

procurement officials should ensure that the basic telecommunications capability supplied by FTS-2000 is preserved in communicating information between and among GOSIP systems. This includes in particular GOSIP "value-added" services. In the future, the GSA may become the GOSIP registration authority and may also provide the top level of GOSIP directory services for Government-wide use.

10.2.2 EDI

EDI (Electronic Data Interchange) standards describe formats for orders, payments, shipments, billing, and other business transactions. It is widely used commercially, but is only starting to see Government use. There are two sets of standards for EDI, as follows: (1) the basic set, which contains interchange control, application control, data segment directory, and functional acknowledgement, and (2) transaction sets, which contain formatted messages.

In the OSI architecture, EDI protocols reside at the OSI Application Layer, and EDI may use some of the Application Layer supporting services. EDI transactions may be transmitted as a body part of a MHS (X.400) message or as a file by the FTAM application. EDI may also be implemented as a user-specific application atop OSI ACSE or Transport services. Agencies should determine their specific requirements for EDI and GOSIP products, and when procuring such products, make sure that the functionality required does not conflict.

10.2.3 RDA and SQL

Remote Database Access (RDA) is an emerging standard governing different access modes for a database model on a number of different systems. This model uses a structured database management system, which involves a data manipulation language called Structured Query Language (SQL). This language governs access to relational data bases. Extensive query and retrieval capability is provided via SQL.

It is possible for the GOSIP and RDA applications to be complementary. In particular, an RDA application could specify the GOSIP FTAM as a choice for transfer of information. It is possible for RDA and GOSIP products to be integrated in the future via the ACSE (see sec. 7). The SQL will likely be a component of the APP.

10.2.4 ODA

Office Document Architecture (ODA) provides for interchange of documents (including text, facsimile and graphics information) which are produced in an office environment. Interchange of ODA documents may be by means of data communications or exchange of storage media. ODA documents may be in processable form, final form, or both. Two document structures are defined by ODA as follows: (1) logical structure (meaning or contents), and layout structure (format).

ODA is a GOSIP advanced requirement, and it is anticipated that ODA functionality will be included in Version 2 of GOSIP. In the interim, agency officials should coordinate procurement of ODA and GOSIP Version 1 products to make sure that no conflicts arise.

10.2.5 ISDN and FDDI

ISDN (Integrated Services Digital Network) and FDDI (Fiber Distributed Data Interface) are GOSIP advanced requirements (as described in sec. 7), and will be included in GOSIP as soon as implementation agreements are developed at the NIST/OSI Workshop and at the North American ISDN Users Forum (NIU-Forum). ISDN and FDDI will also be used in contexts other than OSI; thus, Federal agencies must be aware of the many different roles which ISDN and FDDI technologies may fulfill.

ISDN will be incorporated into GOSIP as a subnetwork technology that may be used to support GOSIP higher-level protocols. Other applications of ISDN are possible, and the NIST has established the NIU-Forum to pursue the development of non-GOSIP applications for ISDN, as well as to reach implementation

agreements required to support OSI protocols.

FDDI will be incorporated into GOSIP as a subnetwork technology that may be used to support GOSIP higher level protocols. FDDI may be used to support other protocols and applications. The NIST and other organizations have active FDDI research programs. Users should expect several new applications of FDDI to appear over the next 5 years.

10.2.6 POSIX

POSIX refers to a standard application interface for portable operating systems which was promulgated in August 1988 as Federal Information Processing Standard 151. Its importance lies in the fact that it is the first attempt to specify a common set of program calls and command line interfaces for an operating system. In the future, many operating systems are expected to offer compliant interfaces and subroutine libraries.

The GOSIP FIPS and POSIX FIPS are complementary, and their effect is expected to be synergistic. The POSIX standard will be used to provide a favorable software development environment for many applications, including OSI protocols. The GOSIP standard will be used to achieve interoperable data communications between computer systems. Furthermore, POSIX will permit portability of applications software. POSIX is expected to be the operating system component of the APP. Federal agencies should ensure in procurements that GOSIP and POSIX requirements are properly integrated. A project is underway to develop a set of GOSIP-compliant protocols for inclusion with a future release of the Berkeley version of UNIX. Efforts have also begun to define network services program calls for POSIX. Users should support these efforts.

10.2.7 Security

The initial GOSIP security specification is limited to a security option for the Connectionless Network Protocol. Work is now underway at the NIST and the National Security Agency (NSA) to develop a set of security protocols for use with GOSIP. The set of such protocols is known as the Secure Data Network Service (SDNS). An outline of the security requirements for GOSIP is given in an appendix to the Version 1 GOSIP FIPS. An initial set of SDNS protocols is aimed at security for the transport and network layers, as well as for the electronic mail application. A key management protocol will also be required.

10.2.8 CALS

CALS (Computer Aided Logistics Support) is a program representing a major effort by the DOD to promote common document formats and information exchange to aid the transfer and modification of blueprints, technical literature and training manuals. The draft standards include draft military specifications for raster graphics and for computer graphics metafiles. There is a CALS 1840A standard and a draft amendment to MIL-D-28000, which is an additional application subset of the Initial Graphics Exchange Standard. In sum, there is a comprehensive set of standards which governs the DOD support of digital information exchange.

The CALS initiative relies heavily on the TOP OSI user specification (see sec. 3), and CALS will use OSI communications protocols to convey the necessary information. Products supporting CALS are emerging, and compliance to CALS standards is being defined.

Close cooperation is being maintained between the two initiatives, and it is expected that this cooperation will continue in the future. The NIST is supporting the DOD actively in the CALS development effort, and intends to ensure that the GOSIP and CALS development efforts are consistent.

10.2.9 GKS, CGM, and PHIGS

The GKS (Graphical Kernel Set) is a high-level applications-oriented interface standard for transmitting graphics information between different systems. This standard has existed for several years, and the NIST is currently registering objects defined under the GKS scope. GKS specifications promote the portability of

graphics applications across different ADP environments.

CGM (Computer Graphics Metafile) specifications ensure a common file format for files containing graphical data. The CGM standard permits transmission and storage of graphics information between different graphical software systems or different graphical devices. This graphical information may be stored in a device-independent manner. The CGM standard is a low-level device-oriented standard that interfaces applications-oriented software to device drivers.

The difference between the CGM and the GKS standards lies in the level of specification, as described above. Both the CGM and the GKS standards are GOSIP advanced requirements. Federal users can consult the GOSIP appendices to determine the latest status of this work in reference to present and future procurement efforts.

The Programmers Hierarchical Interactive Graphics System (PHIGS) standard is a relatively sophisticated hierarchical interface for graphics applications such as simluation, modeling, and computer-aided manufacturing. In general the PHIGS standard is more complex than the GKS standard. The PHIGS standard is not explicitly referenced in the GOSIP Version 1 FIPS.

10.3 General Instructions

Following is advice that should be followed by an agency official when considering various standardization efforts and whether or not they will conflict. In practice, the various standards development groups will have resolved major technical questions in creating the particular processing standard, but agencies may still have concerns about internal application of these standards. Agencies may also have concerns about supplemental or optional OSI services required to properly integrate GOSIP with the above-described work (in particular, other components of the APP).

Federal agencies should:

(1) consult NIST to determine what Federal Information Processing Standards are available and what new technology will be included in GOSIP in the future (by consulting the Appendices in the GOSIP FIPS),

(2) in a long-term OSI acquisition strategy and procurement process, continually monitor the status of emerging Federal standard-setting efforts and include this new work in future procurements, and

(3) designate certain officials to consult with vendors when considering a solicitation to determine any conflicts between an agency's communication requirements and other computer-related requirements, as well as to resolve these conflicts if they arise.

APPENDIX A

OSI TUTORIAL INFORMATION

This appendix gives tutorial and explanatory information on the protocols referenced in the GOSIP Version 1 FIPS. A large amount of technical material is presented as an aid to understanding content of sections of the Users' Guide.

Organization of the appendix is into four sections. The first portion deals with network technologies; the second portion describes the Transport Layer. The third portion describes the FTAM (File Transfer, Access and Management) protocol, and the final portion describes the MHS (Message Handling Systems) protocol. These portions taken together completely describe all layers of the OSI Reference Model.

A.1 Network Technologies Tutorial

This section provides tutorial information on network technologies that are referenced in GOSIP. The first subsection gives a general introduction. Successive subsections describe specialized network designs. For additional material on these topics, please consult appropriate references given in Appendix B.

A.1.1 Introduction

A GOSIP network is composed of different subnetworks which may use different technologies to move data. These subnetworks are connected by intermediate systems which relay messages between different subnetworks and mask the differences in the various technologies. There are four technologies specified in GOSIP as follows: ISO 8802/3 (CSMA/CD), ISO 8802/4 (token bus), ISO 8802/5 (token ring), and X.25 wide area network. CSMA/CD stands for "carrier sense multiple access with collision detection." The ISO 8802/3, 8802/4, and 8802/5 standards are identical to the respective IEEE 802.3, IEEE 802.4, and IEEE 802.5 standards.

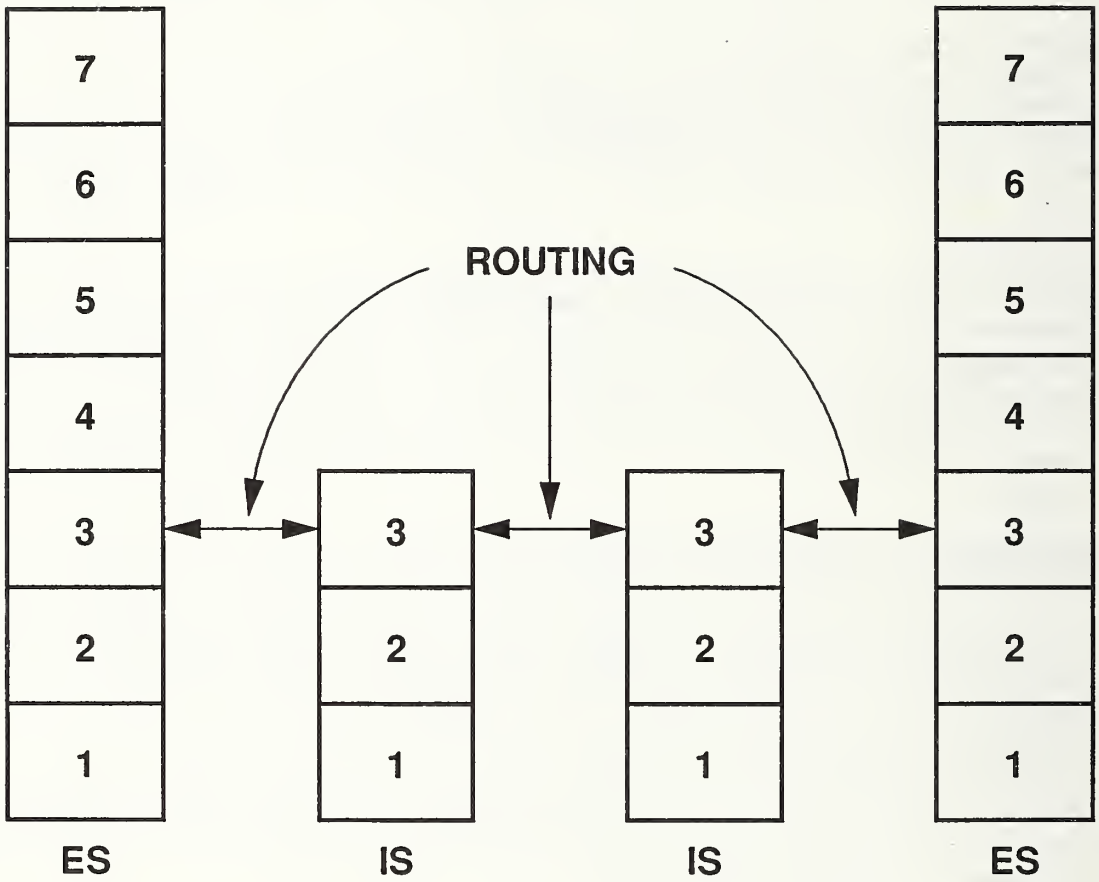
GOSIP applies to both intermediate systems and end systems. Intermediate systems are "middle" systems that interconnect subnetworks. GOSIP protocols from Layers 1 through 3 are contained in intermediate systems. End systems, on the other hand, are terminus systems which originate or receive Transport messages. GOSIP protocols included in end systems are those from OSI layers 1 through 7. Intermediate systems perform routing and relaying of packets between end systems to support the Network Layer service provided by those end systems. Figure 22 illustrates these concepts.

A concern for users in terms of applications effectiveness is to ensure that data has been transferred correctly between end systems, possibly passing through different types of subnetworks, not all of which are equally reliable. This subsection discusses the different technologies incorporated in layers 1-3 (Physical, Data Link, Network) of the OSI Reference Model.

As Figure 23 shows, the GOSIP subnetwork technologies may be architecturally divided into local area networks and wide area networks. Standards development emphasizes certain features of the technologies under consideration, depending on their application. For instance, local area networks have hosts separated by short distances, and wide area networks have hosts separated by longer distances. These local area networks and wide area networks are integrated using the CLNP (Connectionless Network Protocol).

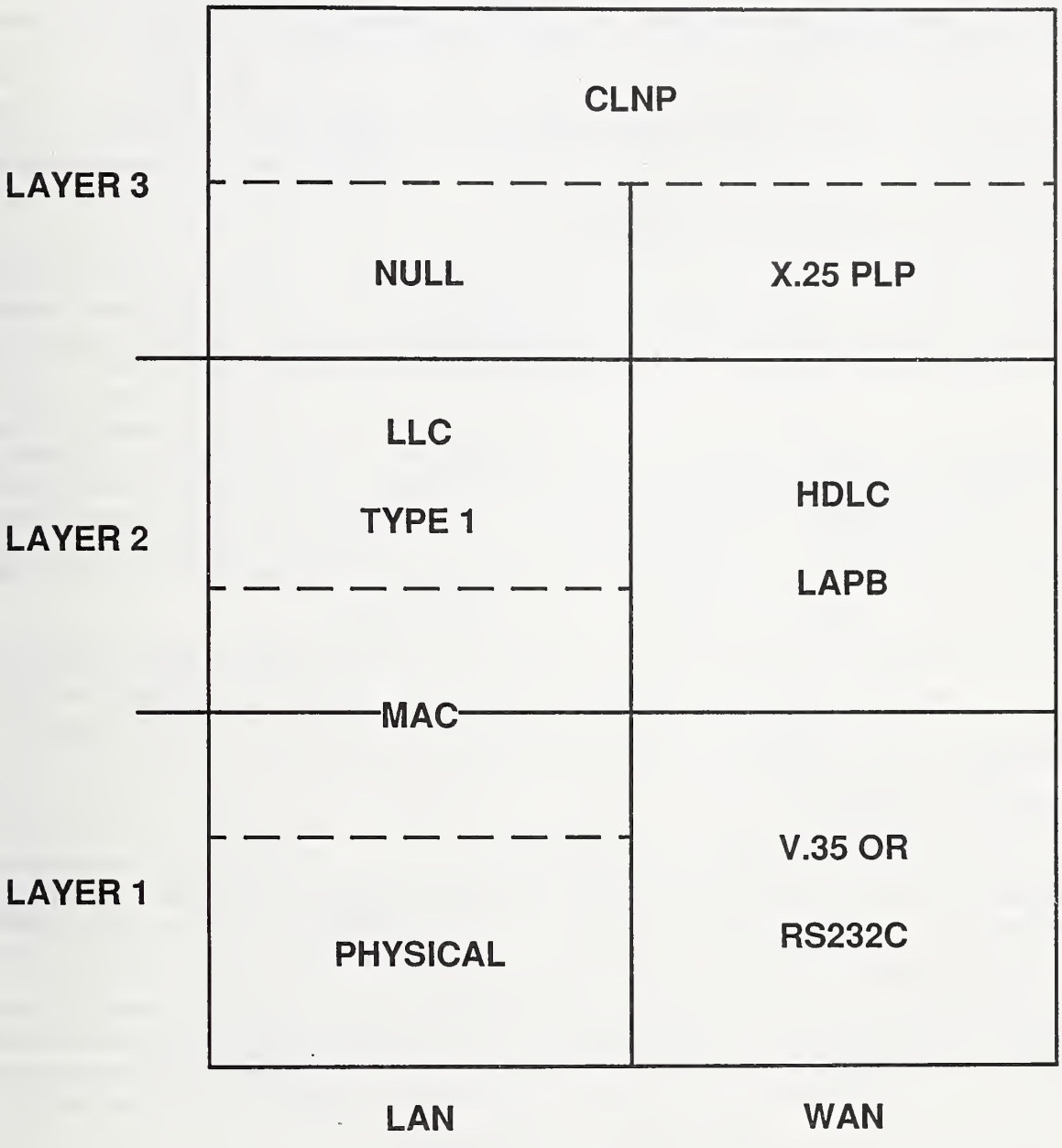
Partitioning of the OSI Physical Layer, Data Link Layer, and Network Layer functionality differs between local area networks and wide area networks, but all of the functional elements of each layer must be included in each technology. Below, layers 1-3 are described in terms of OSI layer functionality. Subsections A.1.2 and A.1.3 describe how the local area network and wide area network standards map into the OSI Model as shown in the columns of Figure 23.

The Physical Layer is capable of transmitting raw bits over a communication channel. The Physical Layer defines the conventions for transmitting and recognizing bits as either 0 or 1. Some concerns of the



ES = END SYSTEM
IS = INTERMEDIATE SYSTEM

FIGURE 22
GOSIP ROUTING SUMMARY



LAN = LOCAL AREA NETWORK
WAN = WIDE AREA NETWORK

FIGURE 23
GOSIP SUBNETWORKS

Physical Layer are how many volts should be used to represent a 1 and how many for a 0, how many microseconds make a bit, whether transmission may proceed simultaneously in both directions, how many pins the network connector has and what the use of each pin is. The types of cable technology used are coaxial cable and twisted-pair, although fiber optic technology is also possible. The Physical Layer provides modulation techniques sufficient to represent a signal across an imperfect cable. It should be noted that the Physical Layer does not guarantee error-free transmission of bits; this is left to higher layers.

The task of the Data Link Layer is to take the raw transmission facility provided by the Physical Layer and transform it into a link that appears substantially free of transmission errors to the Network Layer. It performs this function by taking bits, forming them into data frames and transmitting the frames sequentially. The Data Link Layer provides error detection and correction capability (involving two computers directly connected) across a line between nodes of a subnetwork.

The Data Link Layer checks the number and position of bits received, and performs various calculations to determine if there is an error, e.g., if a "1" bit is accidentally received as a "0". Synchronization of sender and receiver is important in this layer. Both the Physical and Data Link Layers apply only to "box-to-box" communications; that is, management of bits between directly-connected computers.

The Network Layer performs the routing and relaying of data between hosts on the same or different subnetworks. The Network Layer assures that data packets are correctly routed toward the destination end system. The network header is examined by Network Layer entities to determine where to send the packet next Along the way packets may be fragmented. Since different packets and fragments may take routes through different sequences of subnetworks, the packets and fragments may arrive out of order and must be reassembled (placed together) at the destination end system. Although reassembly is a layer 3 function, reordering is a layer 4 (Transport) function which will be mentioned later.

The CLNP assumes a datagram level of service from the subnetworks (either local area networks or wide area networks). Datagram service implies that data packets are sent as individual isolated units, which may arrive out of order, in fragments, or not at all. It is up to a higher layer of functionality (Transport) to ensure in-order, accurate delivery of data between end systems.

A.1.2 Local Area Networks

Three different local area network technologies are discussed below. These incorporate the functionality of the lowest three layers of the OSI Reference Model. There are many different kinds of local area networks; three types have been selected for inclusion in GOSIP because they are generic in applicability, are relatively simple to implement, provide acceptable performance in most instances, and are, in general, widely available.

Local area networks have three distinctive characteristics: (1) a diameter of not more than a few kilometers, (2) a transfer rate exceeding 1 Mbps (megabit per second), and (3) ownership by a single organization. Since distances are short, it is economical to install high-bandwidth cable between hosts. These cables may be divided into channels, where each channel defines a different path of communication.

The GOSIP link layer is composed of the logical link control (LLC) Type 1 sublayer and media access control (MAC) sublayer. The MAC sublayer manages the Physical Layer and mediates access to it by means of an access discipline, e.g., CSMA/CD. The LLC Type 1 sublayer provides a mapping between the LLC Type 1 services and the MAC services.

Frame delivery is provided at locations called LSAPs (link service access points) for local area networks. Datagram service implies the passing of data packets as isolated units, where packets may arrive out of order or not at all.

As referenced in figure 23, the Physical Layer is bundled with the MAC, and the LLC Type 1 provides datagram service to the CLNP above it. The LLC Type 1 provides checksum service. The Physical Layer-MAC combinations are different for each local area network chosen. The interfaces between the physical

medium, the MAC, and the LLC are distinct, but do not always correspond evenly with the functional layer interfaces defined in the OSI Reference Model. This is due to the fact that the local area network standards were originally defined outside of the OSI standardization effort.

Local area networks are distinguished by the method multiple hosts use to compete for a shared cable. Access to this cable may be: (1) deterministic, or (2) random. In deterministic access, there is a predefined scheme by which a host is guaranteed access to a cable. In random access, open competition for the use of the cable occurs, involving any hosts who wish to transmit. The three kinds of local area networks described below include both types of access, and offer advantages or disadvantages depending upon a user's particular requirements and existing configurations.

CSMA/CD is an example of random access networks. An arbitrary number of hosts may be connected to a cable in CSMA/CD. Only one sender can use the cable at one time. A host may attempt to send immediately if desired, without waiting for a predefined signal. Because of a very small propagation delay for a signal on a line, any host connected to the line can "listen" to the line before attempting to use it. If two hosts attempt to use the line at the same time, a collision occurs, and both hosts immediately stop transmitting. Each host tries again later, using a "backoff" algorithm. The retry times computed are likely to be different for each host.

An important implementation of this scheme, the IEEE 802.3 standard, is the basis of the GOSIP-compliant CSMA/CD. There are several minor differences between Ethernet, a precursor, and IEEE 802.3. These differences are in the way the backoff time is calculated, and in one of the link-layer header fields. As mentioned previously, the IEEE 802.3 standard is identical with the IS 8802/3 standard referenced by GOSIP. The IS 8802/3 standard includes both baseband and broadband coaxial cable in the specification.

The principal advantages of CSMA/CD are low cost, simplicity, wide availability, and quick response time in light to moderate traffic loads. The principal disadvantage is a degradation in performance under heavy traffic conditions.

The token bus scheme (IS 8802/4) uses a bus (single cable) architecture like that used by CSMA/CD, with stations connected to the cable. Unlike CSMA/CD, however, the token bus scheme uses a token passed from host to host to regulate access to the cable. An algorithm controls the logical ordering of hosts set to receive the token; this order may or may not be the physical order of hosts on the cable. A host may only send data when it has the token; after finishing the host relinquishes the token to the next host in the logical ordering. Thus, there is no contention for the cable as in CSMA/CD. Token bus schemes typically use broadband transmission on a coaxial cable.

The advantage of the token bus scheme is that it provides regulated access and deterministic performance even under heavy load. The disadvantage is the complexity of the implementation, particularly that of the algorithm used to control host ordering, as well as the resultant high cost. Still, by applying a token bus technology a user is able to derive better performance in a variety of situations than with CSMA/CD. GOSIP adopts the token bus scheme in the IS 8802/4 standard.

The organization of token ring networks is fundamentally different from a CSMA/CD network. In contrast to a carrier sense network which is basically a passive, electrically connected cable onto which all stations tap, a ring network is actually a series of point-to-point cables between consecutive stations. The ordering of activity in a ring network is by the physical order of the stations. The IS 8802/5 technology allows operation on twisted pair and coaxial cable. A host must have the token in order to transmit, and the token ordinarily moves around the ring in round-robin fashion. Timers are used to control token holding time; when a timer expires, the host must relinquish the token.

The advantage of this scheme is that good performance is obtained, even at moderate-to-heavy traffic loads because access to the ring is regulated. Disadvantages are the need for token maintenance and delay in sending even in light traffic conditions. However, for GOSIP users, the token ring approach offers a viable alternative to the other technologies in effectively transferring data between hosts. The GOSIP token ring

technology is based upon the IS 8802/5 standard.

Table 3 summarizes the options and features available to 8802-based local area networks. A comparison of capabilities is thus possible. In table 3, "C" represents coaxial cable technology, "TP" stands for twisted-pair technology, and "NA" stands for "not applicable."

Table 3 - Local Area Network Comparison

LAN=8802/3, BASEBAND=yes, BROADBAND=yes, SPEED=10 Mbps, CABLE TYPE=C

LAN=8802/4, BASEBAND=yes, BROADBAND=yes, SPEED=10 Mbps, CABLE TYPE=C

LAN=8802/5, BASEBAND=NA, BROADBAND=NA, SPEED=5 Mbps, CABLE TYPE=C,TP

A.1.3 X.25 Wide Area Networks

The X.25 protocol is connection-oriented. The source and destination addresses only have to be given at the beginning of a connection. X.25 is used by GOSIP as a subnetwork for long-haul transmission.

For X.25, the Physical Layer specification for GOSIP is typically RS-232-C for line speeds up to 19.2 kilobits per second, and CCITT V.35 for line speeds above 19.2 kilobits per second. The Link Layer of X.25, LAPB (link access protocol-balanced), is responsible for correct transmission of packets between the end system and the DCE (i.e., data circuit-terminating equipment or X.25 packet-switching node). Here packet switching imples the proper routing and relaying of data packets. The LAPB has the following features: (1) it implements a checksum to ensure that end system/X.25 node frame transfers are received correctly, (2) the flow of frames between the end system and node is controlled by a window mechanism, and (3) frames received are acknowledged and incorrectly received frames are retransmitted.

The X.25 Packet Layer Protocol (PLP) operates over LAPB and provides the X.25 virtual circuit (VC) interface. VCs are logical connections between DTE (data terminal equipment) nodes. Since the CLNP assumes a simple datagram interface to its underlying subnetworks, a collection of functions is defined to map between the service assumed (datagram) and the service provided (VC). These subnetwork-dependent convergence functions open X.25 VCs to destinations identified by the subnetwork address passed down from the CLNP with each datagram request, accept VCs from remote systems, pass to CLNP messages received on X.25 VCs, and close VCs when there is inactivity. The subnetwork dependent convergence function thus isolates the CLNP from the specific characteristics of the underlying subnetwork (in this case, that it is connection-oriented).

In general, the boundaries between the Physical Layer, the LAPB, and the X.25 PLP are quite distinct. These boundaries correspond well with layer boundaries defined in the OSI Reference Model.

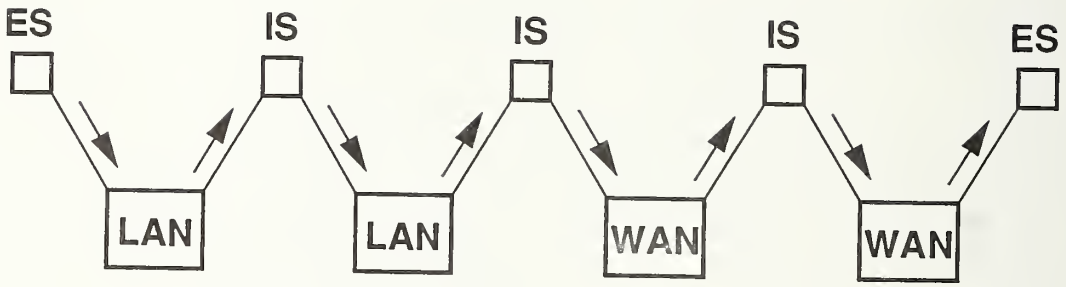
The CCITT X.25 standards have evolved from the 1980 X.25 Recommendation to the 1984 X.25 Recommendation, and the evolution continues to the 1988 X.25 standard. Version 1 of GOSIP references the 1984 X.25 Recommendation. The main difference between 1980-based and later X.25 Recommendations is that later X.25s include all capabilities necessary to establish and maintain connection-oriented network service between users whereas 1980 X.25 requires a special protocol called the SNDCP (subnetwork dependent convergence protocol) to achieve this same level of service.

A.1.4 CLNP (Connectionless Network Protocol)

GOSIP subnetworks may be of different types as described above with different specifications, and for expanded interoperability it is necessary to interconnect them so that an end system on one subnetwork can communicate with an end system on a different subnetwork. The means used in GOSIP to interconnect subnetworks is the CLNP; this protocol provides OSI Network Layer routing between interconnected subnet-

works, in order to move a data packet from source to destination. The CLNP [ISO 13] provides a datagram service to the Transport Layer above, and a datagram service is provided to the CLNP from either a local or wide area network.

The CLNP includes provisions for segmenting data packets for greater efficiency. A "lifetime" feature indicates the number of hops from the source to a given intermediate system, and the reassembly timer gives a time deadline for recreation of complete data packets at the destination end system. Each protocol data unit header contains a destination address, which is used by intermediate systems to route the packet to the correct destination end system. Some other fields in the header are: security, priority, and segment number. The CLNP is typically used to link together different local area networks to create a single larger internetwork, and may be used to link together different wide area networks as well (or to link together a mixture of local area and wide area networks). Figure 24 illustrates this.



ES = END SYSTEM
IS = INTERMEDIATE SYSTEM
LAN = LOCAL AREA NETWORK
WAN = WIDE AREA NETWORK

FIGURE 24
CLNP FUNCTION

A.2 Transport Layer Tutorial

The Transport Layer of the OSI Reference Model provides reliable "end-system-to-end-system" data transfer. There are five classes of Transport service; these are known as Class 0 through Class 4. Some Transport classes (including Class 4) provide retransmission of lost data, flow control, and reordering of data packets. Transport Class 4, which provides the highest level of capability of the five classes defined, is required for GOSIP systems. Transport Class 0 has the lowest level of functionality of the five classes. Generally, there is an increase in functionality with an increase in class number for Transport Classes 0, 2, and 4. Classes 1 and 3 have, in general, not been widely accepted or implemented. The reason that Transport Class 4 was selected for GOSIP is that its use promotes the maximum degree of interoperability between different systems, and that it is required for operation over the CLNP.

A.3 File Transfer, Access and Management (FTAM) Tutorial

This section gives a general description of the services provided by FTAM and what additional capabilities are needed to make it work.

A.3.1 FTAM Protocol, Service, and Model

The File Transfer, Access and Management (FTAM) Standard [ISO 2-5] allows for the effective transmission, access operation, and management capabilities of a variety of different file types and formats across electronic media, without detailed knowledge of the particular charcteristics of the remote machines.

Briefly, FTAM allows different applications or different users of applications to transfer information without specific knowledge of the other system's characteristics. FTAM also allows users a greater degree of control over the file activity, as well as an expanded set of capabilities and features. Futhermore, all of this is accomplished in a completely automated fashion, and in a globally interconnected environment. Other applications may use FTAM as a supporting service. In fact, FTAM can be used locally as a set of callable library routines.

The FTAM standard is composed of four parts: a General Description, a Virtual Filestore, a File Service Definition, and a File Protocol Specification. The General Description deals with basic terminology and broad FTAM concepts, and should be read first. The File Service Definition gives an overview of FTAM services provided to the user, and should be read next. The Virtual Filestore section gives information on the central model used by FTAM, and should be read next. Finally, the File Protocol Specification gives a detailed description of the protocol interactions necessary to accomplish the FTAM activity.

In addition, there are three addenda as follows: overlapped access, filestore management, and protocol conformance. Overlapped access deals with reading to and writing from different portions of a file simultaneously; filestore management involves an extensive set of directory commands, including search, list, and change directory.

Currently, the standard is an IS (International Standard) in the International Standards Organization. The addenda will progress to IS by 1990. Furthermore, the FTAM section in the NIST Workshop Agreements [NIST 1] is based upon the IS FTAM documents. All of the FTAM products marketed by vendors are expected to be based upon the FTAM IS.

The services of FTAM provided to the user are: (1) the ability to communicate about files without specific knowledge of the other system, (2) the facilities to express explicitly what the users require, (3) the ability to specify uniform file properties, (4) the ability to specify record-level file access and positional file transfer, and (5) detailed file management. This list is expected to grow over time as more special-purpose applications are written which may use FTAM as a supporting service.

Some examples of applications which may use FTAM are the following: distributed database management applications, document retrieval and updating (library information services), and specialized "messaging" systems composed of long text messages. Applications which transfer large amounts of structured data reliably end-to-end between heterogeneous systems, large accounting and payroll applications, large inventory control applications, and worldwide automated financial integration systems are also included.

FTAM is a two-party file transfer protocol; in other words, there is a controller of the file activity (initiator) that directs the action, and a responder, that responds to the initiator in a passive role. All file transfers and access operations occur between initiator and responder. Three-party file transfer is a subject of discussion for the future. An FTAM implementation may act as initiator, as responder, or as both.

FTAM is defined in terms of functional units and service classes. Service classes are described in terms of functional units; some of these are mandatory within a service class and some are optional. The functional units in FTAM are kernel, limited file management, enhanced file management, read, write, grouping,

recovery, and restart.

Service classes are: transfer, management, access, transfer and management, and unconstrained. The names indicate the functional capabilities. For functional units, the kernel is the basic set of FTAM capabilities. Limited file management deals with the ability to create, delete, and interrogate properties of files. Enhanced file management deals with the ability to change file properties. Grouping allows concatenations of FTAM requests for efficiency purposes.

There are file attributes and activity attributes. File attributes are globally unique and may be seen by anybody accessing the file. Activity attributes are particular to a connection and are only visible to the user of the connection. Via FTAM, a user may query the values of these attributes and possibly change these values. Table 4 gives a partial list of these attributes.

Table 4 - FTAM Attributes

FILE ATTRIBUTES

filename, permitted actions, contents type,
storage account, date and time of creation,
date and time of last modification, identity of creator,
identity of last modifier, file availability,
filesize, access control

ACTIVITY ATTRIBUTES

active contents type, current access request,
current initiator identity, current location,
current processing mode, current account,
current concurrency control

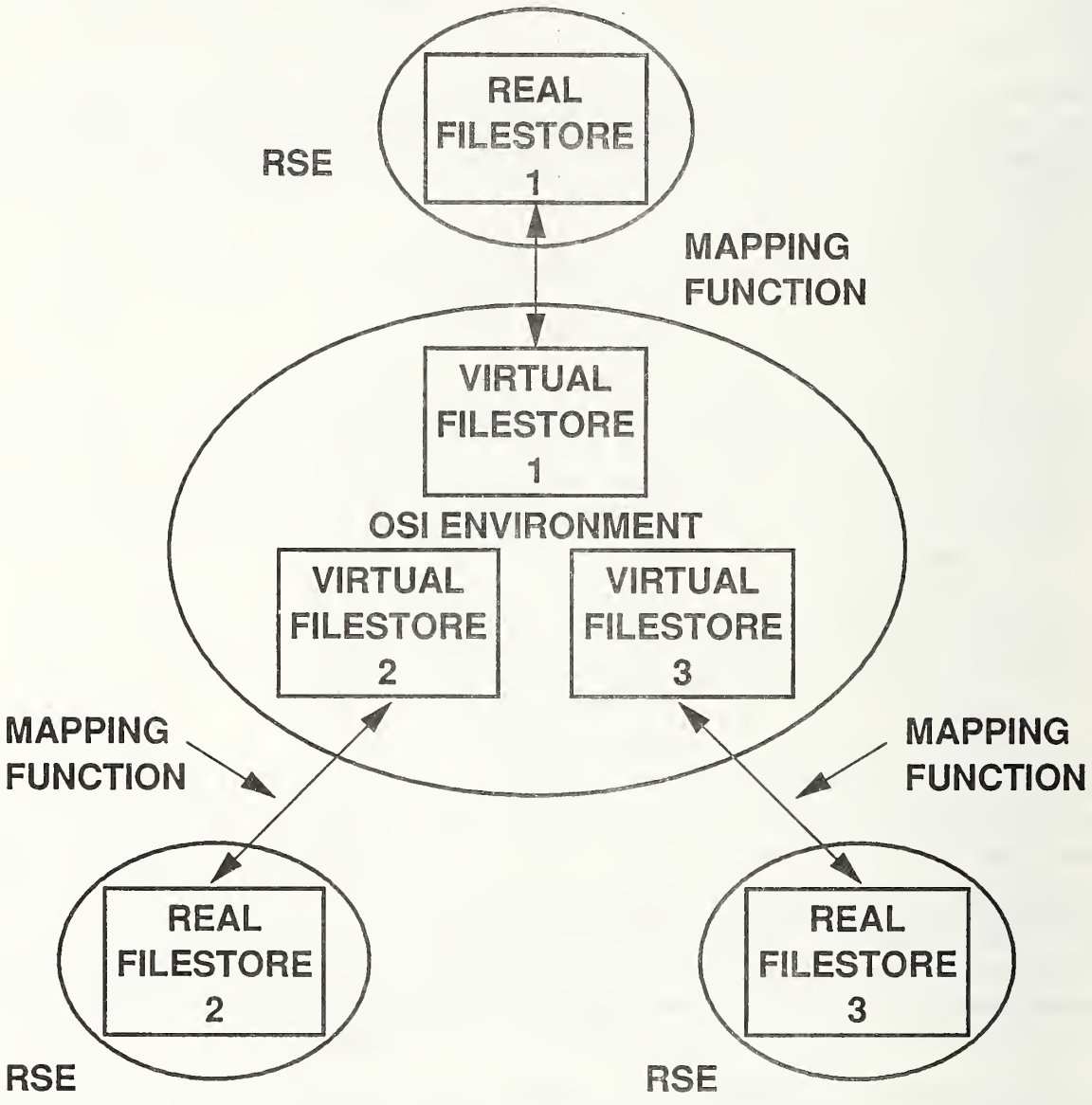
FTAM embodies the concept of a virtual filestore. In the OSI environment, there is one conceptual representation of this virtual filestore model. In the real environment, there are multiple real filestore implementations. Thus there must be mapping between a real filestore and a virtual filestore. The nature of this mapping is a local issue. Figure 25 illustrates this mapping.

The generic FTAM model is applicable to most FTAM systems in use today. All of the characteristics of the virtual filestore can be recognized and interpreted by any OSI file system, so the essence of communication is through this model. As the need for other models occurs in FTAM, they will be developed.

The FTAM service may be described as a series of regimes. Regimes may be defined as environments which may be entered and exited via confirmed services. The first or outermost regime is the application association regime; this involves setting up an FTAM activity within the context of an association. Service primitives involved in this effort are F-INITIALIZE to set up, and F-TERMINATE or F-ABORT to exit. Figure 26 depicts the FTAM regimes.

Once the first regime is entered then filestore management is invoked. This is where file directory services will be available in the near future. Next comes the selection/creation regime. This is the regime where the attributes of a file are specified, for a file already existing on a destination system (F-SELECT), or new attributes of a file are created (F-CREATE). The corresponding service primitives which terminate this regime are F-DESELECT and F-DELETE, respectively. This regime involves specifying the properties of a file.

Once the file selection regime is entered, attributes can be queried or changed. The F-READ-ATTRIB



RSE = REAL SYSTEMS ENVIRONMENT

FIGURE 25
MAPPING BETWEEN REAL SYSTEMS AND OPEN SYSTEMS

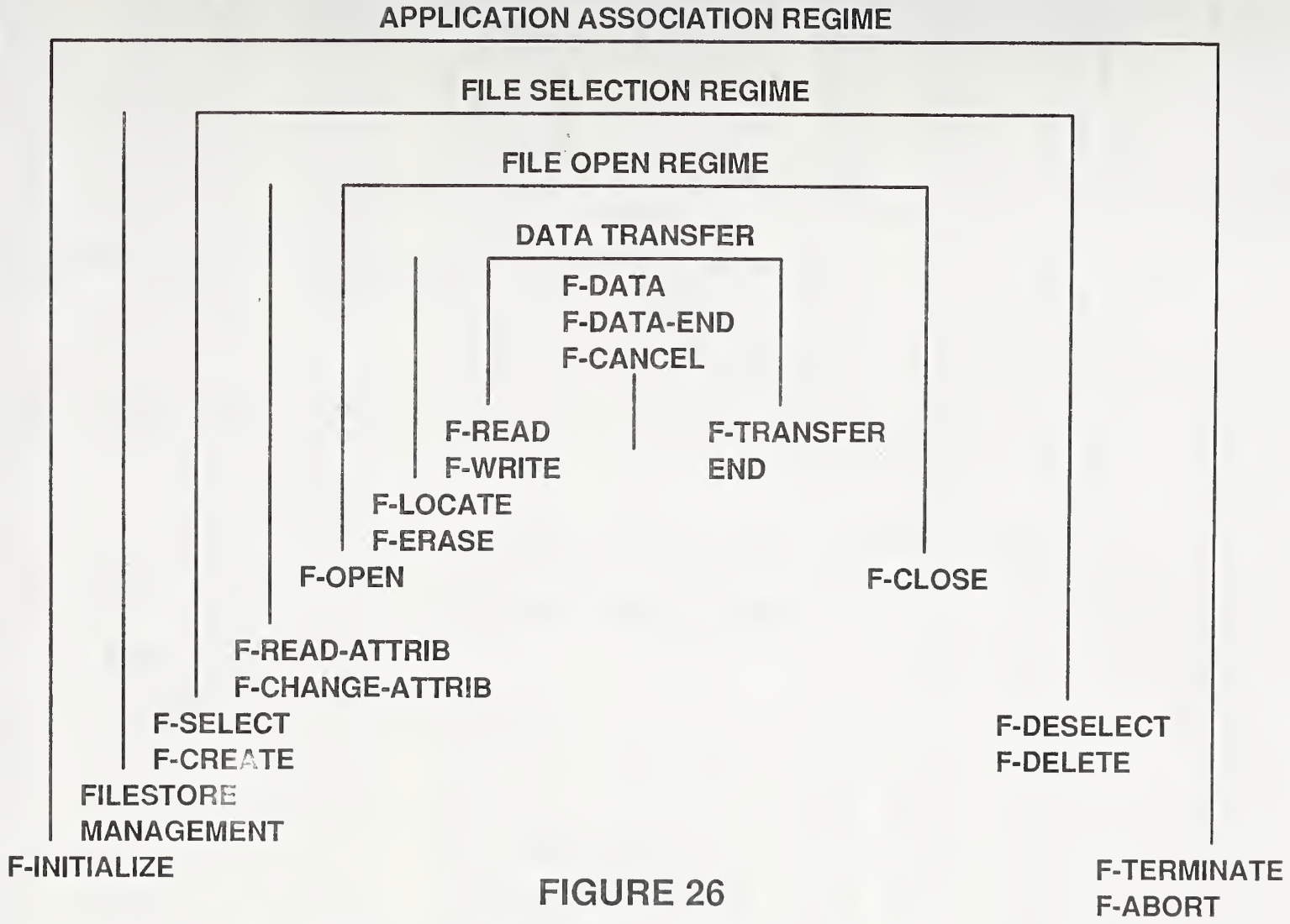


FIGURE 26
FTAM REGIMES

service primitive is used to query attributes. The F-CHANGE-ATTRIB service primitive is used to change attributes.

Next comes the regime where the file is opened; this implies that the file contents may be accessed by the initiator. The service primitive to invoke here is the F-OPEN service primitive. This primitive has a number of important parameters. In the open regime are contained the locate and erase actions. These actions are represented by the LOCATE and ERASE service primitives. The LOCATE action finds a specified record in a file, and the ERASE action removes a specified record.

The next actions to invoke are those of F-READ and F-WRITE; F-READ is used to read the file, and F-WRITE is used to write the file. These actions generally occur in opposite directions. Among the primitives accessed are F-DATA, as well as F-DATA-END and F-CANCEL. F-DATA actually carries the data, F-DATA-END terminates the data, and F-CANCEL cancels the action. The entire data transfer action is completed by an F-TRANSFER service primitive.

F-CLOSE terminates the OPEN regime and makes access to the file contents impossible. The service primitives to abruptly exit from an FTAM activity are F-U-ABORT and F-P-ABORT. F-U-ABORT is issued by either file service user; F-P-ABORT is issued by the service provider.

As mentioned previously, the FTAM model is a two-party model. There is an initiating file service user, who is separated from the FTAM Initiator by a user interface. The FTAM Responder is also connected to a responding file service user by a user interface. Figure 27 illustrates this scenario.

A virtual filestore schema is composed of a: (1) file, which contains file attributes and file contents, (2) filestore, which may contain a number of files, and (3) a connection, which involves active attributes and current attributes. These is a user attached to the connection. The schema is hierarchical with a (tree-like) structure. Specific parts of a file are defined using node identifiers, or File Access Data Unit (FADU) IDs. Many different access structures are possible. For example, one user may wish to view a file as essentially a flat structure, whereas another user may wish to view the file as having a hierarchical structure.

The properties of a virtual filestore are: (1) that it may contain an arbitrary number of files, (2) that the properties of each file are determined by global file attributes, (3) each file is either empty or has some contents and a structure, and (4) at most one file in the virtual filestore is bound to a particular FTAM regime at any one time. Also, a set of activity attributes is associated with each FTAM regime; these are particular to an FTAM activity. An arbitrary number of FTAM initiators may have FTAM regimes at any one time.

FTAM has a rich set of diagnostics, which convey detailed information about the status of an FTAM request. There is provision for users to include additional explanatory material where appropriate. FTAM has four classes of errors, from minor errors to errors which destroy the FTAM activity. Each of these classes is dealt with in an appropriate manner.

FTAM information is conveyed via special messages called service primitives. Each primitive describes a particular action taken by a file service user. These primitives include associated parameters, which are special fields containing common values. Each value has a predefined meaning. The sequence is as follows: first a request is made by one machine. This request is received by the destination machine, which sends back a response (either yes or no) to the request. This response is received by the requester as a "confirm" action.

Each of the service primitives has a list of parameters. These may be mandatory, optional or conditional. For example, for F-INITIALIZE, some parameters are: result, called application title, calling application title, responding application title, presentation context management, service class, functional units, attribute groups, files quality of service, and initiator identity. The parameters have particular values, and the ordering of parameters is important.

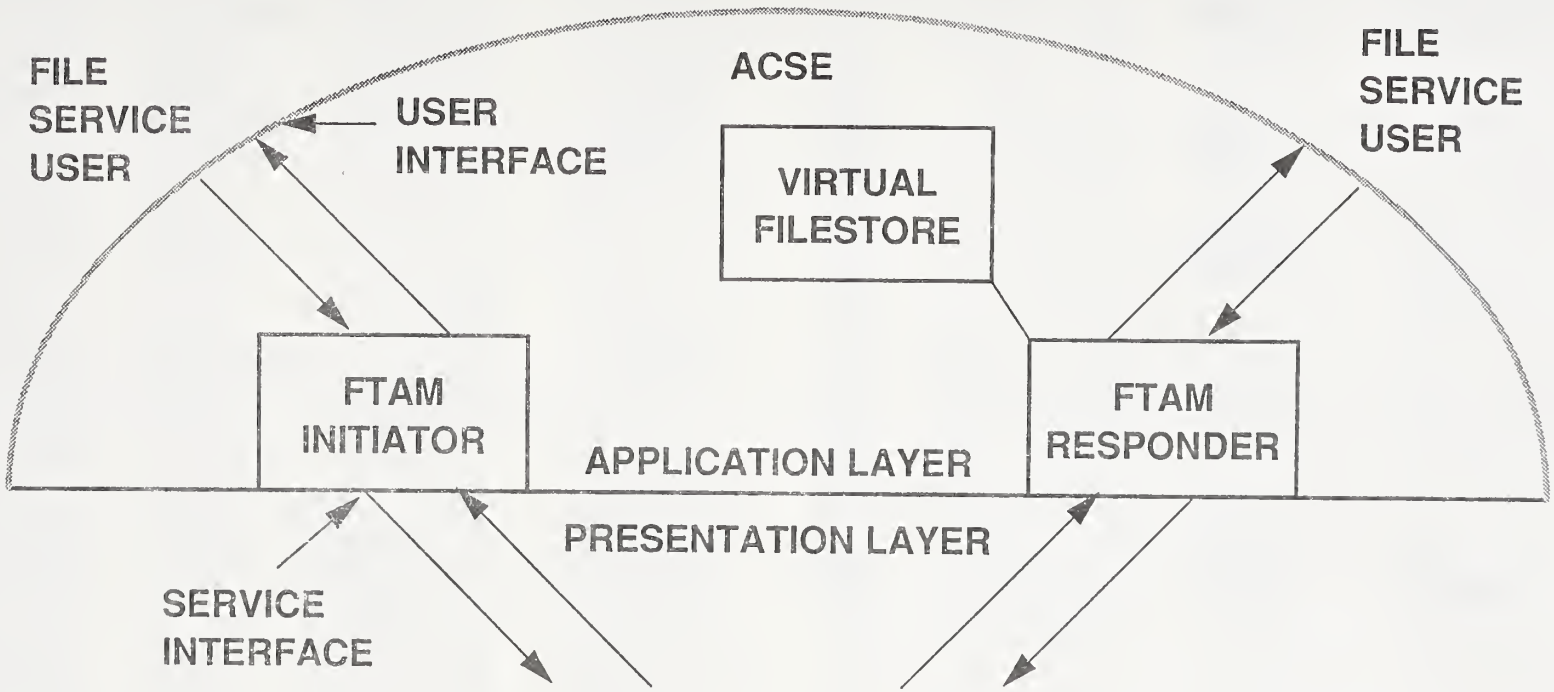


FIGURE 27
FTAM MODEL
(TWO PARTY)

The file access structure of FTAM is described hierarchically. There are various levels to this hierarchy; at each level are nodes, each of which may be connected to zero or one data unit. These nodes could be considered place-holders in a file, and represent locations. A corresponding concept is block or record position in a real file. There is a root node at level 0. The tree organization is hierarchical. A data unit corresponds to a block or record of data in a real file. There is a file access data unit (FADU) at each node, and FADUs encompassing multiple nodes. These FADUs represent (smaller or larger) portiions of the file. Level numbers increase from the root downward; nodes at a fixed level may be siblings, and each node at a fixed level has zero, one or more children at a deeper level (higher level number). Figure 28 illustrates these concepts.

Access control is invoked in many different ways in FTAM. To start, the FTAM user has a set of permitted actions allowed for that user for that activity. Correspondingly, each file has a set of allowable actions attached to it. The FTAM user can only operate at the intersection of these capabilities. The requested access FTAM parameters specify the actions potentially allowable to the FTAM user.

File attributes describe generic properties of a file, and activity attributes describe generically the state or condition of an FTAM connection. In terms of FTAM file attributes and activity attributes, some common file attributes are: filename, permitted actions, contents type, storage account, date and time of creation, identity of creator, filesize, and future filesize. Other file attributes are access control, file availability, and legal qualifications. Some of the common activity attributes are active contents type, current location, current account, current access passwords, and current processing mode.

File types supported in FTAM are: sequential text, indexed sequential, sequential binary, directory, and random-access. Data types supported are: different versions of text (character sets), real (floating-point), integer, and boolean.

There are four types of FTAM information conveyed: FTAM data units, FTAM protocol information, FTAM structuring information, and abstract syntax information. An abstract syntax is the general description of the kinds of information that FTAM uses. It is necessary to convey the structure of an FTAM file before transmitting it between initiator and responder. The means by which FTAM conveys this information is document types and constraint sets.

Document types are specific descriptions of file structure; constraint sets are more general descriptions. For example, for an ASCII sequential text file with 80-character records delimited by CR-LF pairs, a document type name could adequately describe this. However, to describe all text files with sequential record structure, a constraint set name should be used. There are document types defined within the FTAM standard, and document types defined by the workshop. Each document type describes a specific file structure; this information is passed at F-OPEN time.

There is a one-time negotiation between initiator and responder when making any FTAM request. An initiator proposes, and a responder modifies the initiator's request by subsetting it, if necessary. Based upon the nature and characteristics of the request, the responder may accept or reject the request.

Several ISO contraint sets are allowed. Among them are: unconstrained (applies to entire file as atomic unit), sequential flat (simple sequential), ordered flat (indexed sequential), ordered hierarchical (hierarchically organized files with constraints), general hierarchical, and none. The list of ISO document types is divided into: FTAM-1 (unstructured text file), FTAM-2 (sequential text file), FTAM-3 (unstructured binary file), FTAM-4 (sequential binary file), and FTAM-5. Table 5 summarizes these prominent document types.

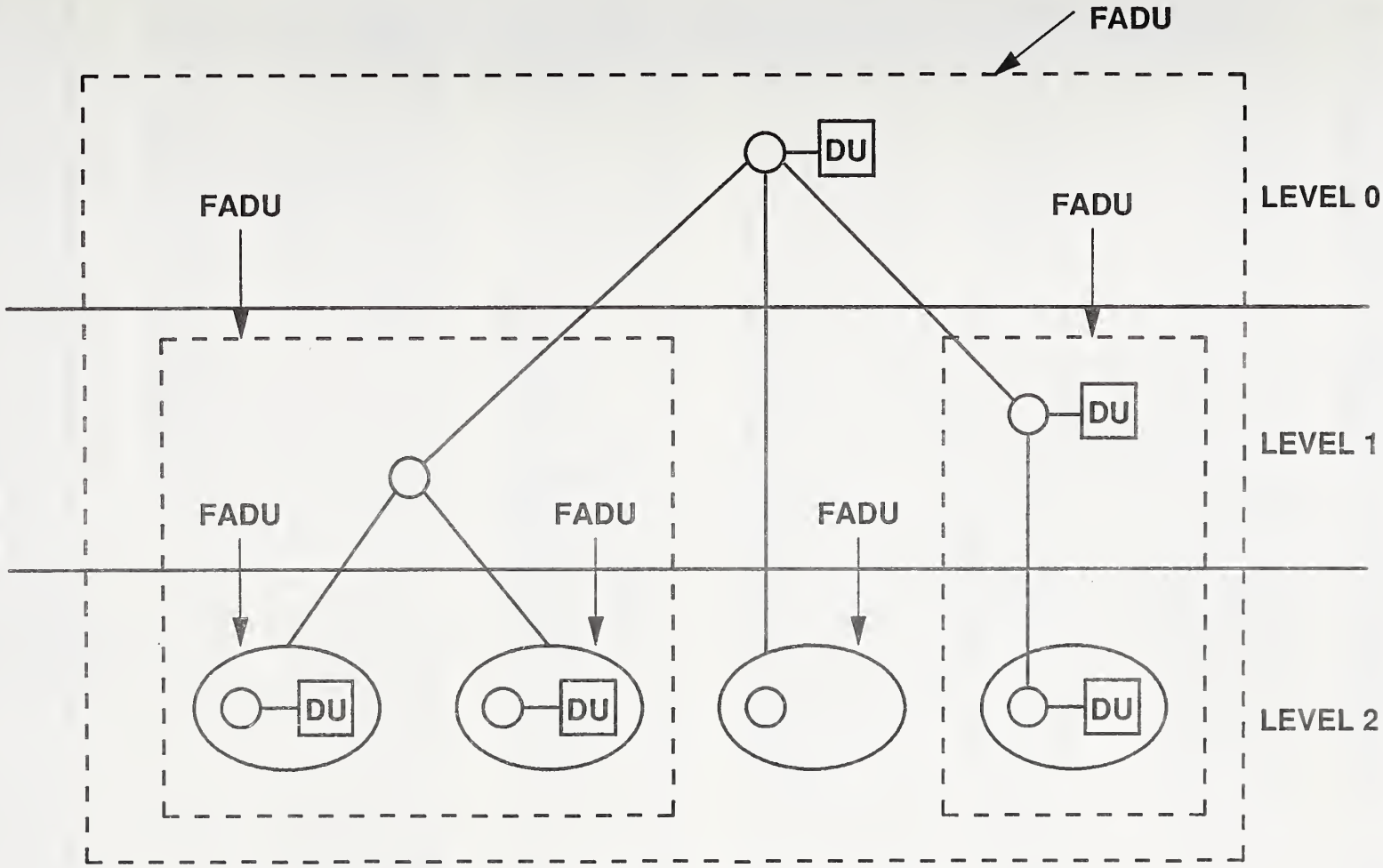


FIGURE 28
FILE ACCESS STRUCTURE

Table 5 - FTAM Document Types

NAME = FTAM-1

DESCRIPTION: unstructured text (a single character string with no delimiters)

==========

NAME = FTAM-2

DESCRIPTION: sequential text (some character strings separated by delimiters in a sequence, and order is important)

==========

NAME = FTAM-3

DESCRIPTION: unstructured binary (a single binary string with no delimiters)

==========

NAME = FTAM-4

DESCRIPTION: sequential binary (some binary strings separated by delimiters in a sequence, and order is important)

==========

NAME = FTAM-5

DESCRIPTION: simple hierarchical (series of records or blocks organized in a tree-like structure) (for example, indexed sequential file)

There are two FTAM service types defined. One is internal; this supports the error recovery protocol. Errors are apparent to the file service user, the user is allowed to directly control error recovery procedures, there are four classes of errors defined, and all the functional units defined in the standard are included. The other is called external; in this situation, the file service user has no awareness of error detection and recovery, it is dependent upon the files quality of service level, and it includes all functional units except restart and recovery.

Three kinds of attributes defined in the NIST Workshop Agreements are: kernel, storage, and security. Each group contains both file and activity attributes. The group titles indicate their functional descriptions. There is limited concurrency control provision within the FTAM agreement. All functional units are supported except restart and recovery.

The NIST Workshop Agreements [NIST 1] have specific information on parameters as well as how information is negotiated. An FTAM implementation may act in any of four roles: initiator-sender, initiator-receiver, responder-sender, and responder-receiver. When data is actually being exchanged, one side is the sender and the other side is the receiver. This is independent of the initiator-responder relationship. In addition, the NIST Workshop Agreements describe Implementation Profiles, which are created so the user

can conveniently specify the functionality required. The Profiles are: simple file transfer, positional file transfer, full file transfer, simple file access, full file access, and management.

These Implementation Profiles are expressed in terms of document types, attributes, and service classes. The Implementation Profiles described in the agreements support the functions of file transfer, file access, and management, and cover all possible situations of interest in basic FTAM capability.

The FTAM Phase Two agreements are upwardly compatible with future FTAM phases, and specify both intiator and responder roles. In addition, these agreements describe both sender and receiver features, support both NIST and FTAM document types, and include concurrency, requested access, and security considerations. The kernel group of attributes is required in these agreements, but all service classes are included.

A.3.2 FTAM Support-Application Layer

The ACSE [ISO 9-10] standards specify a protocol and service common to any application. Since these services of connection establishment and release, as well as identification of source and recipient, are not particular to one application, they were included in a separate standard. This standard is meant to be referenced by all applications, and to provide a framework in which different applications can co-exist.

Application Layer standards define the procedures and the types of information necessary to enable interworking among distributed application processes. The Presentation Layer standards provide mechanisms for defining and selecting the encoding rules for representing the information to be communicated. The data elements defined by the Application Layer standards are abstract definitions of the information to be communicated. It is likely that data elements will be represented "locally" in each system according to different conventions. The conventions for representing information in a computer system are collectively referred to as the syntax of the information. Each system is said to represent the information in its local syntax.

To be meaningful, the procedures and types of information used by application processes to interwork must be encoded according to the same rules. Although it is not necessary that both systems use the same local syntax, it is necessary that they agree on the concrete syntax rules for encoding the information to be transferred. The concrete syntax used in the transfer is called the transfer syntax. In a communication, the transfer syntax may correspond to the local syntax of one or both of the systems involved, or it may be different from that of both systems. What is essential is that both systems agree on the transfer syntax and are capable of transforming information from their local syntax to the agreed transfer syntax.

Association Control Service Elements may be used to perform certain generic functions for the FTAM activity; these functions include setting up an association, terminating an association, and error control. These ACSEs and corresponding FTAM elements are carried by the Presentation Layer protocol.

Other Application Layer standards are important to FTAM besides the ACSE service and protocol. For instance, the emerging CCR (Commitment, Concurrency, and Recovery) standard deals with the following repetitive actions. Commitment specifies the completeness of actions possible on a particular data set, concurrency deals with controlling simultaneous access to a file, and recovery specifies actions necessary to recreate the status of an application activity.

A.3.3 FTAM Support-Presentation Layer

The Presentation Layer standards [ISO 11-12] have mechanisms enabling applications to define and select the transfer syntax for their communication. The Presentation context is negotiated by functions in the Presentation Layer on behalf of the two application processes from the possible set of transfer syntaxes each system can support. During the communication, functions in the Presentation Layer may agree to change the Presentation context, selecting a new one as required by Application Layer standards. The Presentation Layer performs functions that are requested sufficiently often to warrant finding a general

solution for them, rather than letting each user solve the problem.

An example of a transformation service that can be performed at the Presentation Layer is text compression. Most applications do not exchange random binary bit strings; they exchange information such as names or amounts. The Presentation Layer could accept ASCII strings as input and produce compressed bit patterns as output.

The Presentation Layer supports FTAM in terms of establishing and releasing a Presentation context, as well as carrying FTAM and ACSE information between machines. The Presentation address also binds different application processes. Context refers to the syntax in which information is transferred. What the Presentation Layer does for FTAM is to define the allowable syntaxes for FTAM information and control their use.

A.3.4 FTAM Support-Session

The Session Layer provides functions to interconnect or bind two application processes in a logical communicating relationship and to organize and synchronize their dialogue. This is done by providing mechanisms to establish and release Session connections. A Session connection is an agreement between two application processes to engage in a controlled dialogue for the purpose of exchanging data. It is by means of Session connections that application processes can exchange data between them. By the mechanism of the Session connection, application processes can send data and the receiving system can associate it with the intended application process.

The Session connection can be viewed as a connection between the two application processes across the Session Layers of the two end systems. It must be remembered, however, that the Session connection depends on the connection established at lower layers to carry out the Session Layer functions. It depends on these connections to transport data and protocol information. During the connection establishment the two application processes agree on the rules of dialogue to be used in the communication between them. The concept of a dialogue in the Session Layer is similar to that known from human communication. One type of dialogue is characterized by information flowing in only one direction. A second type of dialogue is characterized by a two-way flow of information that is controlled so information flows only in one direction at any given time.

The Session Layer manages the FTAM connection and synchronizes the FTAM data flow. The Session Layer marks (or checkpoints) the FTAM data, so that transmission can restart at a convenient point if an error occurs at the lower layers.

A.4 Message Handling Systems Tutorial

This section gives a general description of the services provided by MHS to the user. For more information, see the References portion of this Guide.

A.4.1 Functional Model

The Message Handling Systems application specified in GOSIP is based on the CCITT 1984 Recommendations. CCITT used the functional model shown in figure 29 to develop those recommendations.

The Message Handling System allows users to communicate by exchanging messages. There are two major MHS components - the Message Transfer System (MTS) and the cooperating User Agents. The Message Transfer System is composed of a series of Message Transfer Agents (MTAs) that are responsible for relaying the message from the originator's User Agent to the recipient's User Agent. The MTA serving the recipient need not be active when the message leaves the originator's MTA; the message can be stored at an intermediate MTA until the recipient's MTA becomes operational. Intermediate MTAs can also perform Application-Layer routing based on address information contained in the message.

The MTAs can be managed by different organizations or administrations. An administration is either the central Postal Telephone and Telegraph (PTT) service in a country or, in the United States, a common carrier recognized by the CCITT. The collection of MTAs and UAs owned and operated by an Administration is called an Administration Management Domain (ADMD). The collection of MTAs and UAs owned and operated by a private organization is called a Private Management Domain (PRMD). Figure 30 shows how PRMDs can cooperate with ADMDs to provide the message transfer service. All ADMDs must comply with the CCITT Recommendations. PRMDs that wish to use a message transfer system provided by an ADMD must comply with the CCITT Recommendations at the point of interconnection.

CCITT has mandated that Transport Class 0 and the Connection-Oriented Network Service (CONS) be used in message systems provided by ADMDs. The NIST Workshop Agreements allow PRMDs to use either Transport Class 0 and CONS or Transport Class 4 and either CONS or the Connectionless Network Layer Protocol (CLNP) at layers 3 and 4. Transport Class 4 and the CLNP are the alternatives most widely implemented in the United States. If a PRMD that does not use Transport Class 0 and CONS wishes to interoperate with an ADMD, a relay MTA containing both Transport and Network Layer implementations must be provided by either the PRMD or the ADMD.

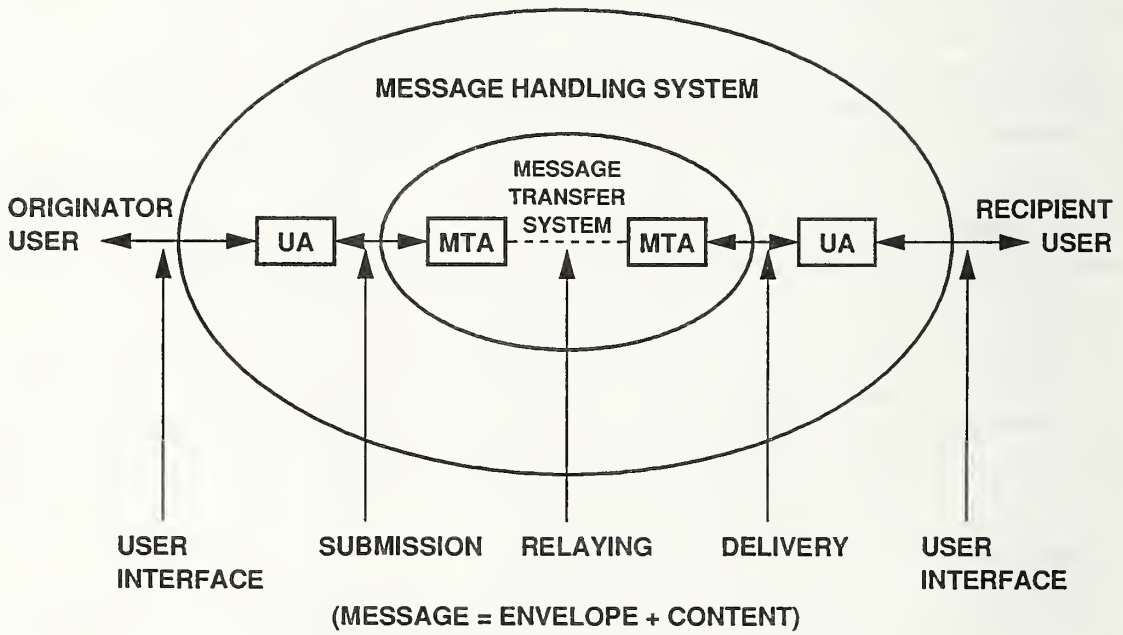
User Agents are the other major components of a Message Handling System. User Agents have many functions that are outside the realm of standardization. The originator's User Agent assists in the creation and editing of a message; the recipient's User Agent stores the message until the recipient chooses to read it and can use certain message fields to determine the display order. However, the message submission and delivery interaction with the MTA must be standardized.

The originator's User Agent must supply to the MTS the message content, the address(es) of the message recipients, and the MTS services that are being requested. The message content is the information that the message originator wants transferred to the message recipient. The address and service request data are placed on the message envelope and used by the MTS to deliver the message.

User Agents can be implemented either in the same system as the MTA or remotely located from the MTA. A remote or stand-alone UA can be under the control of an ADMD, a PRMD vendor, or an organization that provides no message transfer services. Since the UA-MTA message submission and delivery interactions involve a transfer of responsibility for delivering a message, there must be a protocol between the remote UA and MTA to ensure that the transfer of responsibility occurs.

There can be many different types of User Agents. The Message Transfer System can be used to transfer data unrelated to a personal message. It could be a binary bit stream of process control information. As long as the recipient's User Agent can interpret the data sent by the originator's User Agent, meaning-

Reprinted courtesy of
OMNICOM Corporation.



UA = USER AGENT
MTA = MESSAGE TRANSFER AGENT

FIGURE 29
MHS FUNCTIONAL MODEL

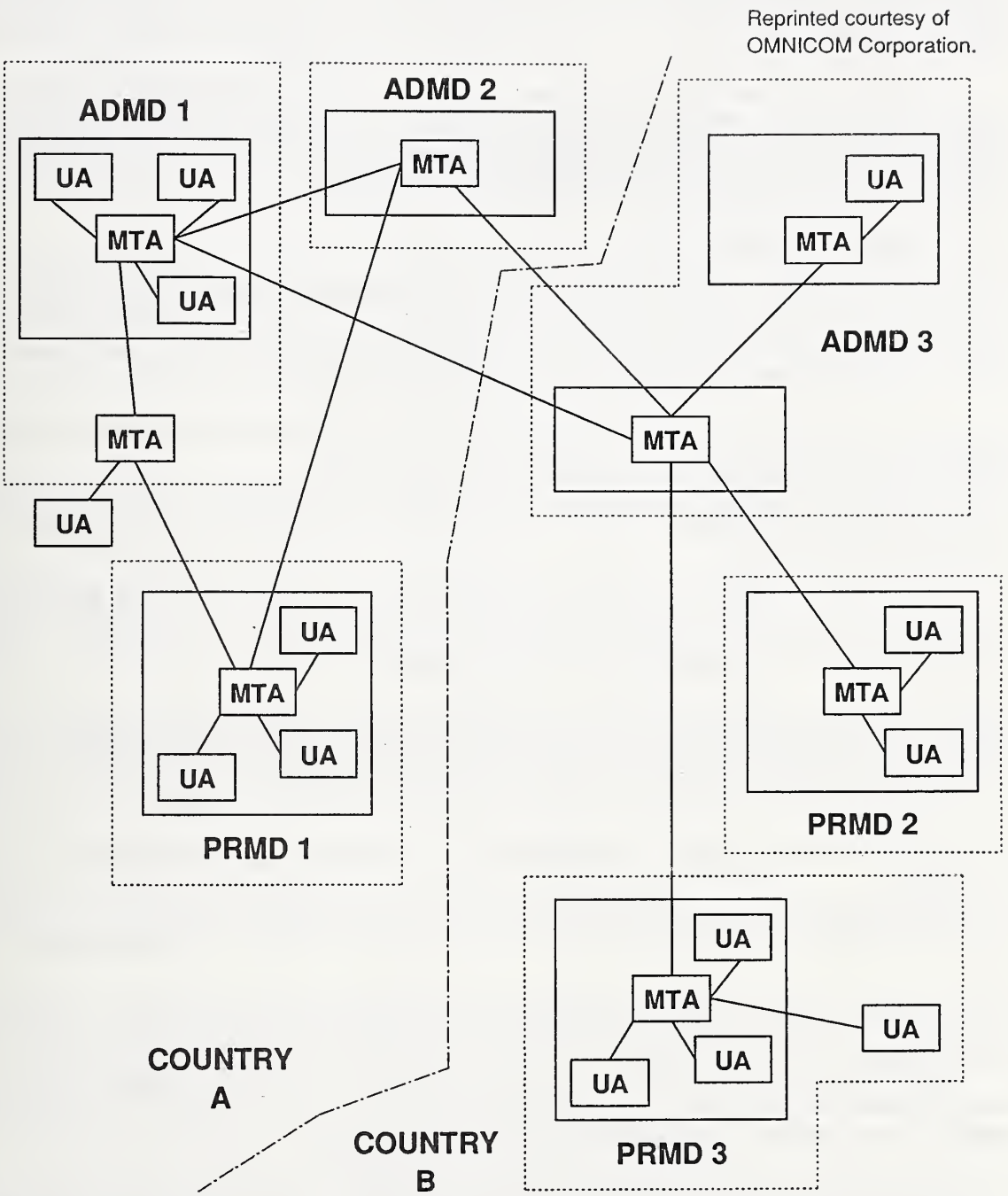


FIGURE 30
X.400 - ADMINISTRATION AND PRIVATE MANAGEMENT DOMAINS

ful communication can occur. The Message Transfer System does not examine the message content unless the User Agent requests that the content be converted from one format to another before delivery. CCITT recognized that, although there were many potential User Agents that could use the message transfer services, the most common use of the Message Transfer System would be to send a personal message from an originator to one or more recipients.

CCITT called the User Agent that provides this service an Interpersonal User Agent and standardized that functionality in the 1984 Recommendations. Although CCITT did not standardize other types of User Agents, they can also use the services of the Message Transfer System as long as they comply with the rules of interaction when submitting or accepting delivery of a message.

A.4.2 Message Transfer System

The Message Transfer System provides basic services to User Agents; these are listed below.

A. Message Identification - A unique ID is assigned to each message. This message ID is used by the MTS to reference messages in delivery and nondelivery notifications.

B. Submission and Delivery Time Stamp - the MTS stamps the time that it accepted responsibility for delivering a message and the time that it fulfilled that responsibility.

C. Non-Delivery Notification - a notification is provided to the originator UA if a message cannot be delivered to any recipient UA.

D. Encoded Information Type Conversion - the originating UA can specify to the MTS the encoded information type of the message being submitted and the MTS can indicate to the recipient UA whether it converted the encoded information when it delivers a message.

E. Content Type Indication- this service enables the originating UA to indicate the content type of the message being submitted. An example of a content type is an Interpersonal Message (IPM).

The service elements below can be selected by the UA on a per-message basis.

A. Multi-destination delivery - the originating UA can request that a message be delivered to more than one recipient.

B. Delivery Notification - the originating UA may request a notification of delivery to each recipient UA.

C. Grade of delivery - three levels of priority processing are provided: normal, urgent, and nonurgent.

D. Deferred delivery - the originating UA may request that a message not be delivered before a certain time. The message is held at the originator's MTA until the delivery time is reached. The deferred delivery request can be cancelled by the originating UA during that interval.

E. Conversion prohibition - the originating UA may prohibit conversion of the encoded information in a message. A non-delivery notification will result if the message cannot be delivered to the recipient UA.

F. Alternate Recipient Allowed - the originating UA can allow this message to be delivered to an alternate UA if there is not an exact match in the Personal Name attribute. The alternate UA is normally a service desk that will manually process the message. The MTS is not required to provide these alternate UAs. If one is not provided, a non-delivery notification will occur.

G. Disclosure of other recipients - the originating UA can instruct the MTS to disclose the names of the other recipients of a multi-recipient message. The originating MTA need not provide the ability to request

this service to the originating UA but, if this service element appears in the message, it must be supported by the recipient MTA.

Additional MTS service elements appear in the CCITT 1984 Recommendations but the NIST Workshop Agreements [NIST 1] do not mandate that they be supported.

A.4.3 Interpersonal Message Service

The Interpersonal Message Service is provided by the class of cooperating UAs called IPM UAs. This service enables a user to send an interpersonal message to one or more recipients and have it received by those recipients. The IPM service is built upon and uses the services of the Message Transfer System.

The interpersonal message contains a header and body. The interpersonal message header contains service elements which facilitate efficient processing of the message by the recipient's UA. The body of the interpersonal message is the information that the message originator wishes to convey to the message recipient. The NIST Workshop Agreements designate the IPM service elements in the interpersonal message header as falling into the following categories.

The service elements below are required in all interpersonal message headers.

A. Interpersonal Message ID - this service element is used by IPM UAs and users to uniquely identify the interpersonal message. The particular method by which this identifier is generated is a local matter. Note that this identifier refers to the message content and is not used by the MTS to reference messages.

B. Originator indication - this service element allows the identity of the originator to be conveyed to the message recipient(s).

The service elements below must be able to be generated upon user request.

A. Primary and Copy Recipients Indication - this service element allows the originator to provide the names of one or more users who are the intended primary and copy recipients of the message. Primary recipients are those who might be expected to act on the message; secondary recipients may be sent the message for information only.

B. Subject Indication - this service element identifies the subject of the message.

C. Replying Interpersonal Message Indication - this service element identifies the message to which this message is a response.

The IPM service need not offer the ability to generate the following service elements to users but if they do appear in an interpersonal message, the receiving UA must recognize them and convey the information to the message recipient. One of the service elements, Blind Copy Request Indication, requires additional processing by the recipient's UA.

A. Authorizing Users Indication - this service element enables the originator to indicate to the recipient the names of one or more persons who authorized the sending of the message.

B. Blind Copy Recipients Indication - this service element allows the originator to provide the names of one or more users who are intended recipients of the message but whose names are not disclosed to either the primary or copy recipients.

C. Cross-Referencing Indication - this service element allows the originator to relate this message to one or more previously sent messages.

D. Obsoleting Indication - this service element allows the originator to indicate that one or more previously sent messages are obsolete.

E. Expiry Date Indication - this service element allows the originator to state the date and time at which the interpersonal message will be obsolete.

F. Reply Request Indication - this service element enables the originator to request that a recipient send an interpersonal message in response to this message. The originator can specify the names of one or more users to whom the reply should be sent and the date by which the reply is required.

G. Importance Indication - this service element allows the originator to indicate his/her assessment of the importance of the message being sent. Three levels of importance are defined: low, normal, and high.

H. Sensitivity Indication - this service element allows the originator to specify guidelines for the relative security of the message upon its receipt. Three levels of sensitivity are defined as follows:

Personal (the interpersonal message is sent to the recipient as an individual, not because of the position that the recipient has in an organization),

Private (the interpersonal message contains information that should be seen only by the recipient), and

Company-confidential (the interpersonal message contains information that should be handled according to company security procedures).

I. Auto-Forwarded Indication - an auto-forwarded message is one that has been forwarded by a recipient UA without user intervention. A new-header encapsulates the original message. This service element allows the recipient to determine that auto-forwarding has taken place and can be used by the recipient UA to prevent additional auto-forwarding and thus act as a loop control mechanism.

Additional IPM service elements appear in the CCITT 1984 Recommendations but the NIST Workshop Agreements do not mandate that they be supported.

A.4.4 Naming and Addressing

In the context of electronic mail, a name is the term by which originators and recipients of messages identify each other. An address identifies an entity by specifying where it is, rather than what it is. An address has characteristics that help the MTS locate the recipient UA's point of attachment.

A name is formed by specifying a set of attributes and the associated values of those attributes. Table 6 gives an attribute list that can uniquely identify a user of the Message Handling System:

Table 6 - MHS Attribute List

Country = United States

Organization Name = ABC Corporation

Personal Name = John Taylor

The address of the message recipient consists of information required to deliver the message to an MHS implementation on a particular end system plus the information needed by the MHS implementation to deliver the message to the recipient's User Agent. The MHS implementation address includes the NSAP address plus the TSAP and SSAP selectors. The Personal Name attribute can be used alone or in conjunction with other attributes to locate the recipient's User Agent.

The CCITT has developed a standard for a directory service to perform the name-to-address mapping [CCITT 10]. An International Standard for directory services is expected from ISO in 1989 [ISO 14].

However, directory service products are not expected until 1990. In the interim, a method of performing the name-to-address mapping is needed.

The solution is to think of an address as a name that contains attributes that are used to locate the message recipient. Name attributes normally consist of information that the originator knows about the potential recipient of a message. Address attributes describe the architecture of the MTS and may be harder for users to remember but they can be used to route the message to the correct MTA.

Table 7 gives an example of how architectural attributes can be applied to the attributes in table 6 to assist in the message routing.

Table 7 - MHS Architectural Attributes

Country = United States

Administration Name = Public Mail System X

Private Domain Name = Private Mail System Y

Organization Name = ABC Corporation

Personal Name = John Taylor

APPENDIX B

ADDITIONAL OSI REFERENCES

Information provided in this Appendix consists of additional references for OSI standards ard related material, and where to obtain this documentation. Agencies may use the addresses indicated to order this information, or it may be ordered from OMNICOM, Inc. at the address below.

OMNICOM, Inc.
115 Park Street, SE
Vienna, VA 22180
(703) 281-1135

Material is presented in this Appendix by group (i.e., CCITT, ISO), and by particular subjects or layers within a group (i.e., Network Layer, Transport Layer). References appearing in the REFERENCES section of this Users' Guide do not appear in this Appendix. For ISO and CCITT references, information is current as of January, 1988. This is not a complete list of OSI-related material; for additional sources of information, contact any one of the organizations given in this Appendix.

CCITT
(Consultative Committee for International Telegraph and Telephone)

Layer-Independent

CCITT Recommendation X.200, (Red Book, 1984), Reference Model of Open Systems Interconnection

Data Link Layer

CCITT Recommendation X.212, Data Link Service Definition for CCITT Applications

Network Layer

CCITT Recommendation X.213, Network Service Definition for CCITT Applications

Transport Layer

CCITT Recommendation X.214, Transport Service Definition for Open Systems Interconnection for CCITT Applications.

CCITT Recommendation X.224, Transport Protocol Profile for Open Systems Interconnection for CCITT Applications.

Session Layer

CCITT Recommendation X.215, Session Service Definition for Open Systems Interconnection for CCITT Applications.

CCITT Recommendation X.225, Session Protocol Profile for Open Systems Interconnection for CCITT Applications.

Presentation Layer

CCITT Recommendation X.216, Presentation Service Definition for Open Systems Interconnection for CCITT Applications.

CCITT Recommendation X.226, Presentation Protocol Profile for Open Systems Interconnection for CCITT Applications.

Application Layer

CCITT Recommendation X.217, Service Definition for the Association Control Service Element

CCITT Recommendation X.227, Protocol Specification for the Association Control Service Element

CCITT Recommendation X.218, Reliable Transfer, Part 1. Model and Service Definition

CCITT Recommendation X.228, Reliable Transfer, Part 2: Protocol Specification

CCITT Recommendation X.219, Remote Operations, Part 1: Model, Notation, and Service Definition

CCITT Recommendation X.229, Remote Operations, Part 2: Protocol Specification

CCITT Recommendation X.501, The Directory, Part 2. Information Framework

CCITT Recommendation X.511, The Directory, Part 3: Access and System Services Definition

CCITT Recommendation X.518, The Directory, Part 4: Procedures for Distributed Operation

CCITT Recommendation X.519, The Directory, Part 5: Access and System Protocols Specification

CCITT Documents may be obtained from:

International Telecommunications Union
Place des Nations, CH 1211
Geneva 20, Switzerland

or

United Nations Bookstore
Room GA 32B
United Nations Plaza
New York, NY 10017

==========

EIA (Electronic Industries Association)

Physical Layer

Interface Between Data Terminal Equipment and Data Communication Equipment Employing Serial Binary Data Interchange, EIA-232D

Application Layer

Manufacturing Messaging Service for Bi-directional Transfer of Digitally Encoded Information, Part 1: Service Specification, RS 511, 1986

Manufacturing Messaging Service for Bi-directional transfer of Digitally Encoded Information, Part 2: Protocol Specification, RS 511, 1986.

==========

IEEE (Institute of Electrical and Electronics Engineers, Inc.)

Media Access Control (Physical Layer)

IEEE Standard for Local Area Networks: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) and Physical Layer Specification, ANSI/IEEE Standard 802.3 - 1985, Institute of Electrical and Electronic- Engineers, 345 East 47th St., New York, NY 10017, 1985.

IEEE Standard for Local Area Networks: Token-Passing Bus Access Method and Physical Layer Specification, ANSI/IEEE Standard 802.4 - 1985, Institute of Electrical and Electronics Engineers, 345 East 47th St., New York, NY 10017, 1985.

IEEE Standard for Local Area Networks: Token-Ring Access Method, ANSI/ISEE Standard 802.5 -

1985, Institute of Electrical and Electronics Engineers, 345 East 47th St., New York, NY 10017, 1985.

Data Link Layer

IEEE Standard for Local Area Networks: Logical Link Control, ANSI/IEEE Standard 802.2 - 1985, Institute of Electrical and Electronics Engineers, 345 East 47th St., New York, NY 10017, 1985.

==========

ISA (Instrumentation Society of America)

Instrumentation Society of America: Proway-LAN, ISA-S72.01, 1985.

Proposed Instrumentation Society of America Standard: Process Control Architecture, dS S72.03, 1987.

==========

ISO (International Organization for Standardization)

Layer-Independent

Information Processing Systems - Open Systems Interconnection - Reference Model, ISO 7498-3, Naming and Addressing.

Information Processing Systems - Open Systems Interconnection - Reference Model, ISO 7498-4, Management Framework.

ISO DP 9646, OSI Conformance Testing Methodology and Framework

ISO DP 9834, Procedures for Specific OSI Registration Authorities

Physical Layer

ISO 2110, 25-Pin DTE-DCE Interface Connector and Pin Assignments

ISO 4902, 37-Pin DTE-DCE Interface Connector and Pin Assignments

ISO 4903, 15-Pin DTE-DCE Interface Connector and Pin Assignments

ISO 2593, 34-Pin DTE-DCE Interface Connector and Pin Assignments

ISO 8481, DTE to DTE Physical Connection Using X.24 Interchange Circuits With DTE-Provided Timing

Data Link Layer

ISO 8886, Data Link Service Definition

ISO 3309, High-Level Data Link Control (HDLC)-Frame Structure

ISO 4335, HDLC - Consolidation of Elements of Procedures

ISO 7776, HDLC - Description of the X.25 LAPB-compatible DTE Data Link Procedures

ISO 7809, HDLC-Consolidation of Classes of Procedures

ISO 7478, Multi-Link Procedures

ISO 8885, HDLC - General Purpose XID Frame Information Field Content and Format

ISO 1745, Basic Mode Control Procedures for Data Communication Systems

ISO 1177, Character Structure for Start/Stop and Synchronous Character Oriented Transmission

ISO 2629, Basic Mode Control Procedures - Conversational Information Message Transfer

ISO 8802-1, Local Area Networks, Part 1: Introduction

Network Layer

Information Processing Systems-Open Systems Interconnection-Network Service Definition, IS 8348

Information Processing Systems-Open Systems Interconnection-Addendum to the Network Service Definition Covering Connectionless Data Transmission, IS 8348/AD1

Information Processing Systems-Open Systems Interconnection-Addendum to the Network Service Definition covering Network Layer Addressing, IS 8348/AD2

Information Processing Systems-Open Systems Interconnection-Internal Organization of the Network Layer, IS 8648

Information Processing Systems-Open Systems Interconnection-Addendum to IS 8473-Provision of the Underlying Service Assumed by ISO 8473, ISO TC 97/SC 6 N 3453

Information Processing Systems-Open Systems Interconnection, Working Draft, End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with ISO 8473 ISO TC 97/SC 6 N 4053

Information Processing Systems-Open Systems Interconnection-Data Communication-X.25 Packet Level Protocol for Data Terminal Equipment, IS 8208

ISO 8878, Use of X.25 to Provide the Connection-Oriented Network Service

ISO DIS 8880, Protocol Combinations to Provide and Support the OSI Network Service

Transport Layer

Information Processing Systems-Open Systems Interconnection-Transport Service Definition, IS 8072

Information Processing Systems-Open Systems Interconnection-Transport Protocol Profile, IS 8073

Session Layer

Information Processing Systems-Open Systems Interconnection-Session Service Definition, IS 8326

Information Processing Systems-Open Systems Interconnection-Session Protocol Profile, IS 8327

Presentation Layer

Information Processing Systems-Open Systems Interconnection-Profile of Abstract Syntax Notation One (ASN.1), IS 8824

Information Processing Systems-Open Systems Interconnection-Profile of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), IS 8825

7-bit Coded Character Set for Information Processing Interchange, ISO-646

Information Interchange - Representation of Local Time Differentials, ISO 3307

Application Layer-VTP

Information Processing Systems-Open Systems Interconnection-Virtual Terminal Service-Basic Class, IS 9040

Information Processing Systems-Open Systems Interconnection-Virtual Protocol-Basic Class, IS 9041

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 1: General Information, DIS 8613/1

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 2: Document Structures, DIS 8613/2

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 3: Document Processing Reference Model, DIS 8613/3

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 4: Document Profile, DIS 8613/4

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 5: Office Document Interchange Format, DIS 8613/5

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 6: Character Content Architecture, DIS 8613/6

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 7: Raster Graphics Content Architecture, DP 8316/7

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 8: Geometric Graphics Content Architecture, DP 8613/8

Application Process–Computer Graphics–CGM/GKS

Information Processing Systems-Computer Graphics-Metafile (CGM) for the Storage and Transfer of Picture Description Information, Part 1: Functional Specification, IS 8632/1

Information Processing Systems-Computer Graphics-Metafile (CGM) for the Storage and Transfer of Picture Description Information, Part 2: Character Encoding, IS 8632/2

Information Processing Systems-Computer Graphics-Metafile (CGM) for the Storage and Transfer of Picture Description Information, Part 3: Binary Encoding, IS 8632/3

Information Processing Systems-Computer Graphics-Metafile (CGM) for the Storage and Transfer of Picture Description Information, Part 4: Clear Text Encoding, IS 8632/4

Information Processing Systems-Font and Character Information Interchange, IS 9541

Information Processing Systems-8-bit Single Byte Coded Graphic Character Sets, Part 1: Latin Alphabet Part 1, IS 8859/1

Information Processing Systems-Computer Graphics Functional Specification of the Graphical Kernel System (GKS), IS 7942

Information Processing Systems-Computer Graphics-Graphical Kernel System for Three Dimensions (GKS-3D), Functional Description, DIS 8805

Information Processing Systems-Computer Graphics-Programmers Hierarchical Interactive Graphics System (PHIGS), DP 9592

Information Processing Systems-Computer Graphics-Interfacing Techniques for Dialogues with Graphical Devices (CGI), ISO TC 97/SC 21 N1179

Other Application Layer

ISO DP 9545, Application Layer Structure

ISO DIS 9804, Definition of Application Service Elements - Commitment, Concurrency, and Recovery

ISO DIS 9805, Specification of Protocols for Application Service Elements - Commitment, Concurrency, and Recovery

ISO DP 9595, Management Information Service Definition

ISO DP 9596, Management Information Protocol Specification

ISO DIS 9594-2, The Directory, Part 2: Information Framework

ISO DP 9579, Remote Database Access

ISO DIS 9066-1, Reliable Transfer, Part 1: Model

ISO DIS 9072, Remote Operations

ISO documents may be obtained from:

ANSI
ISO TC 97/SC 6 Secretariat
1430 Broadway
New York, NY 10018

==========

NIST (National Institute of Standards and Technology)

Local Area Networks: Baseband Carrier Sense Multiple Access with Collision Detection Access Method and Physical Layer Profiles and Link Layer Protocol, FIPS 107, NTIS, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161

Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Operation With Packet-Switched Data Communications Networks, FIPS 100, NTIS, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161

Implementation Agreements Among Participants of OSINET, National Institute of Standards and Technology, NBSIR 86-3478-7

Implementation Guide for ISO Transport Protocol, National Institute of Standards and Technology, ICST/SNA-85-18, 1985

Franx, C.;Mills, K., Open Systems Interconnection for Real-Time Factory Communications: Performance Results, Workshop on Factory Communications, National Institute of Standards and Technology, NBSIR 87-3516, 1987

NIST FIPS documents may be obtained from:

NTIS
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22181

Other NIST documents may be obtained from:

National Institute of Standards and Technology
National Computer Systems Laboratory
Gaithersburg, MD 20899

APPENDIX C

GOSIP REGISTRATION FORMS

The three forms contained herein are to be used by agencies to register the appropriate GOSIP identifiers. Agencies should send the appropriate forms to the addresses indicated. Copies may be made for multiple requests.

X.400 PRIVATE MESSAGE BODY PART REQUEST FORM

Requestor Provides:

What the number will identify (be as specific as possible):

Number Assigned:

Requestor's Name:

Title:

Organization:

Address:

Phone Number:

Date Needed:

Return form to:

Group Leader (X.400)
Program Coordination and Support
National Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

FTAM DOCUMENT TYPE REQUEST FORM

Requestor Provides:

What the number will identify (be as specific as possible):

Number Assigned:

Requestor's Name:

Title:

Organization:

Address:

Phone Number:

Date Needed:

Return form to:

Group Leader (FTAM)
Program Coordination and Support
National Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

NSAP ORGANIZATION ID REQUEST FORM

Requestor Provides:

Organization Name (up to 64 characters):

Number Assigned:

Requestor's Name:

Title:

Organization:

Address:

Phone Number:

Date Needed:

Return form to:

Group Leader (ORG ID)
Program Coordination and Support
National Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

ADPENDIX D

NIST/OSI WORKSHOP PARTICIPANTS LIST

This Appendix gives a list of organizations participating in the NIST/OSI Workshop. The goal of this Workshop is to develop implementation agreements based upon emerging recognized international OSI standards. This list is arranged alphabetically, and includes both vendors, users, and other interested parties.

This list is taken from participant registrations according to NIST records since January 1987. If a participant has registered at least once for any Workshop during this period, that participant's organization should be represented on this list. NIST does not represent this list as being complete in fact; omissions from this list represent an oversight and are regretted.

LIST OF WORKSHOP PARTICIPANTS

ADCU/WE, Aeronautical Radio, Allied Technologies, Ameritech, Analytic Sciences, Apollo, Apple Computers, Applied Technologies, ARINC Research, Arthur Anderson, ASR Group, AT and T, Australian Ministry of Defense, Automated Office Systems, Bank of America, BBN Communications, Bechtel, Bell Atlantic, Bell Canada, Bell Communications Research, Bell Northern, Bell Southern, BNR, Boeing, Booz Allen, Bridge Communications, British Telecom, Canon, Carnegie-Mellon, Case Communications, CCTA, CDSI, Chipcom, Communication of European Community, Comsat, Computer Consoles, Concord, Contel, Control Data, Convergent Technologies, Codex, COS, Cray Research, CSC, CSIRO, CTA Incorporated, D and F Communications, Danish Standards Association, Danish Telecom, Data Connection, Data General, Datapoint, Datatrend, DCEC, DEC, Defense Communications Agency, Defense Logistics Agency, Department of Agriculture, Department of Defense, Department of Education, Department of Energy, DGM and S, Dialcom, Eagle Technologies, Eastman Kodak, EDS, Electricite de France, Enlon, Excelan, FAA, FBI, Federal Judicial Center, Fisher, Ford Aerospace, Foxboro, Gartner, General Dynamics, General Motors, General Services Administration, George Washington University, Global Technologies, Graphnet, Grumman, GTE, Harris, Hewlett-Packard, Honeywell, House Committee on Science, Hughes, IBM, IBM-Italy, ICE, ICL, ICOT, Intel, Illinois Bell, Industrial Technology Institute, Interlan, Itautec, ITC/CMU, James Madison, JRM DND, Korea Telephone Company, Kwangson, Lantron, Lawrence Livermore Laboratory, Linkware, Lincoln National Information Service, Lockheed, Logica, Los Alamos, McDonnell-Douglas, Martin Marietta, Mandex, MCI, MICOM-I, Microtech, Mitech, Mitre Corporation, Modicon, Motorola, NARDAC, NASA, National Research Computer, Naval Data Services, Naval Oceanographic Office, Naval Research Laboratory, NAVTASC, Navy, NBI, NCR Comten, Netwise, Network Systems Corporation, NIST, Nixdorf, NOAA, Northern Telecom, Northrop, NOSC, NSA, NTI, NYNEX, OAO Corporation, OMNICOM, Panadyne, Planning Research Corporation, Prime Computers, Protocomm, Pyramid, Relational Technologies, Renex, Retix, Rockwell, Science Applications, Ship Star, Siemens, Southwest Bell, SRA Corporation, SRI International, Stanford University, Sun Microsystems, Swedish Institute of Technology, Swedish Telecom, Sydney, TASC, Tandem, Telecom, Telematica, Telenet, Texas Instruments, 3COM, Touch Communications, Transportation Services Institute, TRW, UK Department of Trade and Industry, UK Ministry of Defense, Ungermann-Bass, Unified Technologies, Unisys Corporation, University of Delaware, University of Maryland, University of Michigan, University of Wisconsin-Madison, U.S. Air Force, USAISEC, U.S. Army, U.S. House of Representatives Information Systems, U.S. Systems, U.S. Treasury Department, U.S. West, Van Dyke, Verilin, Veterans' Administration, Wang Laboratories, Wellfleet, Western Union, Wollongong, Xerox, Yankee Group, Yokogama

APPENDIX E

USERS' GUIDE EVALUATION FORM

The form contained herein contains a list of comments, questions and suggestions on this GOSIP Users' Guide. Readers of this Guide are encouraged to fill out this form and send it to the Chief, Systems and Network Architecture Division, National Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899 (ATTN: GOSIP USERS' GUIDE COMMENTS). All comments received will be considered for future revisions of the GOSIP Users' Guide, and all comments are greatly appreciated.

GOSIP USERS' GUIDE
READER RESPONSE FORM

1. What did you like most about this Guide?

2. What did you like least about this Guide?

3. What information in this Guide did you find most helpful?

4. What specific suggestions do you have for improvements to this Guide?

NAME

ADDRESS

PHONE

REFERENCES

National Institute of Standards and Technology

1. NBS Special Publication 500-150, Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 1. This document can be purchased from the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402. Stock Number 003-02838-0, Phone Order (202) 783-3238.

2. Government Open Systems Interconnection Profile (GOSIP), Version 1, FIPS 146, August 1988, NTIS, Springfield, VA 22161.

International Organization for Standardization

1. Information Processing Systems - Open Systems Interconnection - Basic Reference Model, Ref. No. ISO 7498-1984(E).

2. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 1: General Introduction, ISO 8571/1, (ISO TC97/SC21 N2331).

3. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 2 The Virtual Filestore Definition, ISO 8571/2, (ISO TC97/SC21/N2332).

4. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 3: File Service Definition, ISO 8571/3, (ISO TC97/SC21/N2333).

5. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 4: File Protocol Specification, ISO 8571/4, (ISO TC97/SC21/N2334).

6. Information Processing Systems - Local Area Networks- Part 3: Carrier Sense Multiple Access with Collision Detection, IS 8802/3.

7. Information Processing Systems - Local Area Networks - Part 4: Token Passing Bus Access Method and Physical Layer Specifications, IS 8802/4.

8. Information Processing Systems - Local Area Networks - Part 5: Token Ring Access Method and Physical layer Specifications, IS 8802/5.

9. Information Processing Systems - Open Systems Interconnection - Service Definition for Association Control Service Element: Association Control, ISO 8649, (ISO TC97/SC21/N2326).

10. Information Processing Systems - Open Systems Interconnection - Protocol Specification for Association Control Service Element: Association Control, ISO 8650, (ISO TC97/SC21/N2327).

11. Information Processing Systems - Open Systems Interconnection - Connection- Oriented Presentation Service Definition, ISO 8822, (ISO TC97/SC21/N2335).

12. Information Processing Systems - Open Systems Interconnection - Connection- Oriented Presentation Protocol Specification, ISO 8823, (ISO TC97/SC21/N2336).

13. Information Processing Systems - Open Systems Interconnection - Protocol for Providing the Connectionless Network Service, IS 8473, N3998, March 1986.

14. Information Processing Systems - Open Systems Interconnection - The Directory - Overview of Concepts, Models and Services, IS 9594, December 1988.

15. OSI Basic Reference Model - Part 2: Security Architecture. ISO/DIS 7498-2 TC 97/SC 21/N1895. Project 97.21.18. May 1987.

The above documents may be obtained from:

ANSI Sales Department
1430 Broadway
New York, NY 10018
(212) 642-4900

Consultative Committee for International Telegraph and Telephone

1. CCITT Recommendation X.25-1984, Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode on Public Data Networks.

2. CCITT Recommendation X.400 (Red Book, 1984), Message Handling Systems: System Model-Service Elements.

3. CCITT Recommendation X.401 (Red Book, 1984), Message Handling Systems: Basic Service Elements and Optional User Facilities.

4. CCITT Recommendation X.408, (Red Book, 1984), Message Handling Systems: Encoded Information Type Conversion Rules.

5. CCITT Recommendation X.409 (Red Book, 1984), Message Handling Systems: Presentation Transfer Syntax and Notation.

6. CCITT Recommendation X.410, (Red Book, 1984), Message Handling Systems: Remote Operations and Reliable Transfer Server.

7. CCITT Recommendation X.411 (Red Book, 1984), Message Handling Systems: Message Transfer Layer.

8. CCITT Recommendation X.420 (Red Book, 1984), Message Handling Systems: Interpersonal Messaging User Agent Layer.

9. CCITT Recommendation X.430 (Red Book, 1984), Message Handling Systems: Access Protocol for Teletex Terminals.

10. CCITT Recommendation X.500, The Directory - Overview of Concepts, Models, and Services, December 1988.

The above documents may be obtained from:

International Telecommunications Union
Place des Nations
CH 1211
Geneve 20 SWITZERLAND

Miscellaneous

1. Manufacturing Automation Protocol, General Motors Corporation, Manufacturing Engineering and Development, Advanced Product and Manufacturing Engineering Staff (APMES), APMES A/MD-39, GM Technical Center, Warren, MI 48090-9040.

2. Technical and Office Protocols, Specification Version 3.0, MAP/TOP Users Group, One SME Drive, PO Box 930, Dearborn, MI 48121.

3. National Research Council, Executive Summary of the NRC Report on Transport Protocols for the Department of Defense Data Networks, RFC 939, February 1985.

Department of Defense

1."Military Standard File Transfer Protocol," MIL-STD-1780, May 1984, Department of Defense, Washington, DC 20301.

2."Military Standard Simple Mail Transfer Protocol," May 1984, Department of Defense, Washington, DC 20301.

3. Memorandum, 2 July 1987, D.Latham, Subject: OSI Policy.

☆ U.S. GOVERNMENT PRINTING OFFICE: 1989—242 -200 / 05055

NBS-114A (REV. 2-8C)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET (See instructions)	1. PUBLICATION OR REPORT NO. NIST/SP-500/163	2. Performing Organ. Report No.	3. Publication Date August 1989

4. TITLE AND SUBTITLE

Government Open Systems Interconnection Profile Users' Guide

5. AUTHOR(S)

Tim Boland

6. PERFORMING ORGANIZATION (If joint or other than NBS, see instructions)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
(formerly NATIONAL BUREAU OF STANDARDS)
U.S. DEPARTMENT OF COMMERCE
GAITHERSBURG, MD 20899

7. Contract/Grant No.

8. Type of Report & Period Covered

Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (Street, City, State, ZIP)

Same as item #6

10. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 89-600749

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)

This document provides guidance to users concerning implementation of the Government Open Systems Interconnection Profile (GOSIP) Federal Information Processing Standard. Information in this document will help users to better understand and employ the GOSIP FIPS. This document will be updated no more than once per year.

12. KEY WORDS (Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)

applicability; evaluation; GOSIP; procurement; registration; transition

13. AVAILABILITY

☐ Unlimited

☐ For Official Distribution. Do Not Release to NTIS

☒ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

☐ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES

146

15. Price

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SYSTEMS TECHNOLOGY

Superintendent of Documents,
Government Printing Office,
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Institute of Standards and Technology Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published quarterly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW., Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NIST research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NIST publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency Reports (NISTIR)—A special series of interim or final reports on work performed by NIST for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Institute of Standards and Technology
(formerly National Bureau of Standards)
Gaithersburg, MD 20899